

Mu'tah University
College of the Graduate Studies

Managing of Computer Emergency esponse Plan for the Central Agency of Information Technology (Kuwait)

By
Mohammed Jassim Al-Yaqoub

Supervised by
Prof. Mustafa Muheilan

Co-Superviser
Dr Saif Al-Nawiseh

A Thesis Submitted to the College of the Graduate Studies in Partial Fulfillment of the Requirements for the Degree of Master in Engineering Management at Industrial Systems Engineering Department / College of Engineering

Mu'tah University, 2016

الآراء الواردة في الرسالة الجامعية لا تُعبر
بالضرورة عن وجهة نظر جامعة مؤتة

بسم الله الرحمن الرحيم



MUTAH UNIVERSITY
College of Graduate Studies

جامعة مؤتة
كلية الدراسات العليا

نموذج رقم (14)

قرار إجازة رسالة جامعية

تقرر إجازة الرسالة المقدمة من الطالب محمد جاسم سعدون اليعقوب الموسومة بـ:

Mainaging of computer emergeney response plan for the central agency of information technology(kwuit)

استكمالاً لمتطلبات الحصول على درجة الماجستير في **ادارة هندسية**.

القسم: النظم الصناعية.

	التوقيع	التاريخ	
أ.د. مصطفى محمد محيلان		30/3/2016	مشرفاً ورئيساً
د.سيف عناد النوايسة		30/3/2016	عضواً
أ.د.عمر نواف المعايطه		30/3/2016	عضواً
د.يزيد أحمد السبوع		30/3/2016	عضواً
د.منذر عبدالرحمن عبدالهادي		30/3/2016	عضواً



عميد الدراسات العليا

د. محمد المحاسنة

MUTAH-KARAK-JORDAN
Postal Code: 61710
TEL :03/2372380-99
Ext. 5328-5330
FAX:03/ 2375694
e-mail: dgs@mutah.edu.jo sedgs@mutah.edu.jo
http://www.mutah.edu.jo/gradest/derasat.htm

مؤته – الكرك – الاردن
الرمز البريدي :61710
تلفون :99-03/2372380
فرعي 5328-5330
فاكس 03/2 375694
البريد الالكتروني
الصفحة الالكترونية

ACKNOWLEDGEMENTS

First and foremost, endless thanks to Allah who gave me the strength and well to complete this thesis.

I would like to express my thanks and gratitude to my mother who gave me the motivation to continue my Postgraduate studies and my wife and life partner. I would like to express my deepest gratitude to my supervisors, Prof. Dr. Eng. Mustafa Muheilan, and Dr. Eng. Saif Al-Nawiseh, who gave me the golden opportunity to do this work. I especially would like to thank my friend and life brother Mohammad baidas, my colleague and friend Khaled Al-Hatem I would also like to thank my friends, who helped me in finalizing this thesis within the limited time frame.

Mohammed Jassim Al-Yaqoub

DEDICATION

To the most precious person in my life, my mother.

Mohammed Jassim Al-Yaqoub

Table of Contents

List of Figures

List of Tables

List of Appendices

List of Abbreviations

aeCERT	United Arab Emirates Computer Emergency Response Team
AP-CERT	Asia-Pacific Computer Emergency Response Team
AusCERT	Australian Computer Emergency Response Team
BCM	Business Continuity Management
CAIT	Central Agency for Information Technology
CERT	Computer Emergency Response Team
CERT.br	Computer Emergency Response Team Brazil
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIRT	Computer Incident Response Team
CMU	Carnegie Mellon University
CSIRC	Computer Security Incident Response Capability
CSIRT	Computer Security Incident Response Team
CSRC	Computer Security Response Center
DHS	Department of Homeland Security
DNS	Domain Name Service
DRP	Disaster Recovery Planning
FIRST	Forum of Incident Response and Security Teams
ENISA	European Union Agency for Network and Information Security
GCC	Gulf Cooperation Council
GCC-CERT	Gulf Cooperation Council CERT
ICT	Information and Communications Technology
IP	Internet Protocol
IT	Information Technology
ictQATAR	Information and Communications Technology of Qatar
IoT	Internet of Things
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
KPI	Key Performance Indicator
KW-CERT	Kuwait Computer Emergency Response Team
LEA	Law Enforcement Agency
NIC.br	Network Information Center of Brazil
OIC-CERT	Organization of the Islamic Cooperation CERT
PoC	Point of Contact
Q-CERT	Qatar Computer Emergency Response Team
SD	Standard Deviation
SEM	Standard Error of the Mean
TF-CSIRT	Task Force of Computer Security Incident Response Teams

TRA	Telecommunications Regulatory Authority
VOIP	Voice over IP
US-CERT	United States Computer Emergency Readiness Team
WWW	World Wide Web

Abstract

Managing of Computer Emergency Response Plan for the Central Agency of Information Technology (Kuwait)

Mohammed Jassim Al-Yaqoub
Mutah University, 2016

This study will show how to implement and manage a computer emergency response team (CERT) in the State of Kuwait. Hence, there is an urgent need to acquire and implement the best practices of CERTs around the world, which protect information systems and services. This stems from the fact that such systems and services are of paramount importance to the social and economic welfare and development of any nation, as they form the main foundation of modern infrastructure. Hence, the security and availability of such systems and services is essential.

Making Kuwait a financial and cultural capital is considered a key priority for all government institutions. To materialize this vision, secure and intrusion-safe systems must be developed, along with a framework to protect sensitive information. The Central Agency for Information Technology (CAIT) has taken the responsibility of administration and protection of such information as well as transportation through the Kuwait's communication infrastructure. CAIT is obliged to protect Kuwait's information repository from non-authorized use, whether disruptive or not, gain the confidence of its users and constituents, and assure the continuity of safe information systems in both governmental and private organizations. Hence, CAIT has embarked on the Kuwait Computer Emergency Response Team (KW-CERT) initiative in order to build the organizational and technical competencies that set the information security standards, policies, and governance requirements.

The objective of this study is to support and implement the KW-CERT initiative, using the best practices and solutions.

الملخص

إدارة خطة طوارئ الحاسوب الخاصة بالجهاز المركزي لتكنولوجيا المعلومات في الكويت

محمد جاسم اليعقوب

جامعة مؤتة، 2016

هذه الدراسة ستتناول كيفية تنفيذ وإدارة فريق الاستجابة لطوارئ الحاسوب (CERT) في دولة الكويت. حيث أن هناك حاجة ملحة لإنشاء مركز لطوارئ حاسبات خاص بدولة الكويت من خلال تطبيق أفضل الممارسات العالمية في هذا المجال، وذلك لحماية أنظمة وخدمات المعلومات. هذه الأنظمة والخدمات ذات أهمية عالية فهي تشكل حجر الأساس الرئيسي للبنية التحتية الحديثة والتي بدورها تضمن تحقيق الرفاه الاجتماعي والاقتصادي والتنمية في أي أمة، وبالتالي فإن توفير مثل هذا المركز والخدمات أمر ضروري.

ان جعل الكويت عاصمة مالية وثقافية تعتبر حاجة ملحة لجميع المؤسسات الحكومية. لتجسيد هذه الرؤية، يترتب الحفاظ على المعلومات المنتقلة خلال الشبكات والمعلومات المحفوظة من التخريب. ومن هذا المنطلق وضع الجهاز المركزي لتكنولوجيا المعلومات (CAIT) على عاتقة حماية هذه المعلومات وضمان استمرارية أنظم المعلومات في كل مؤسسات الدولة باستخدام أحدث طرق وأساليب الوقاية من خلال طرح مبادرة إنشاء المركز الكويتي لطوارئ الحاسوب.

الهدف من هذه الدراسة هو دعم وتنفيذ مبادرة KW-CERT، وذلك باستخدام أفضل الممارسات والحلول.

Chapter 1

Introduction

Introduction

1.1 Background and Motivation

The recent development and innovation in the field of information and communications technologies (ICT) has created a platform for worldwide connectivity. In addition, the evolution of the Internet and equipping all objects in the world with unique identifiers for data transfer over geographically distributed networks and systems has led to the creation of what is currently known as the *Internet-of-Things* (IoT) (Internet of Things Council, 2015) and (IBM, 2015). Potentially billions of devices are now wirelessly connected to the Internet, offering numerous services, covering a variety of protocols, domains and applications. In fact, it is expected that not less than 30 billion devices will be interconnected globally soon (ABI Research, 2013). For instance, hospitals may monitor the conditions of patients, life support devices and even pacemakers from long distances. In addition, factories may automatically tackle production line issues remotely, and people as well as objects may be ubiquitously located. Figure 1-1 shows the technology reach as a function of time with potential applications.

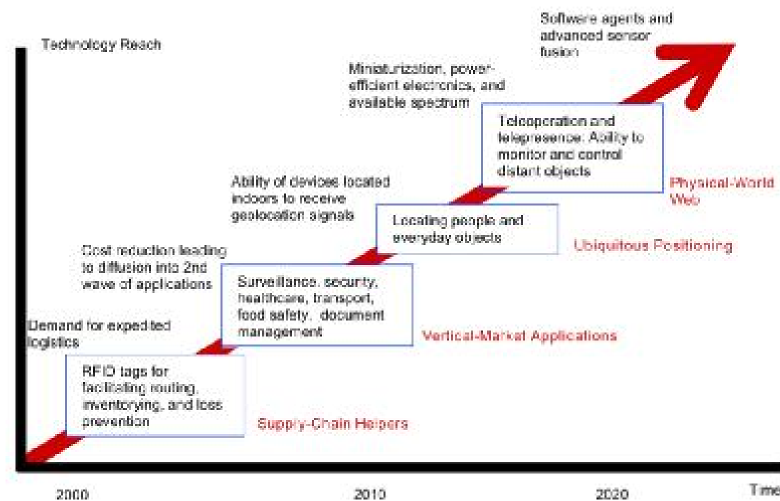


Figure 1-1

Technology Roadmap - Internet of Things (Source: SRI Consulting Business Intelligence (**SRI Consulting Business Intelligence. (2014)**

Many businesses and enterprises have recently evolved their data centers to include *virtualization and cloud computing* infrastructures to improve resource utilization, accelerate development and deployment of services and products (Intel IT Center, 2013). Specifically, in cloud computing systems, local computers no longer have to do all the processing

and handling of transactions and operations. Instead, a network of computing hardware machines, connected through the Internet (and thus making up the "cloud" – Figure 1-2) and run using an interface software such as a Web Browser, are used for intensive data processing and management, ultimately improving business processes and operational efficiency (Buyya, Broberg and Goscinski, 2011).

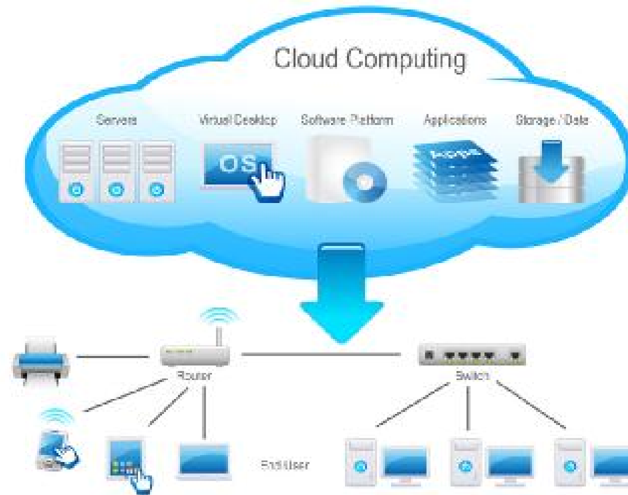


Figure 1-2
Example of Cloud Computing (Source: Cloud Computing in India, 2013)

Unfortunately, every new technological development usually comes with security threats and vulnerabilities that businesses and consumers will inevitably face. Specifically, any device-with embedded operating system-connecting to the Internet may potentially be compromised, eventually becoming a backdoor for attackers into mainframes, servers, desktops of public and private enterprises' networks and data centers. Data stored on such networks may be corrupted or destroyed, as per the following possible attacks (Microsoft TechNet, 2015).

1) *Eavesdropping:* An attacker may gain access to data paths in the network and listen in the traffic. Specifically, data can be read and interpreted as it traverses the network.
2) *Data Modification:* Tampering with the data in transit without the knowledge of the sender or receiver.
3) *Identity Spoofing (IP Address Spoofing):* An attacker may construct internet protocol (IP) packets that appear to have originated from valid addresses within the enterprise's intranet or network services and potentially causing traffic to be diverted to another computer.
4) *Password-Based Attacks:* By gaining access to a network with a valid account, an attacker may modify server and network

configurations, and access other propitiatory information and classified documents.

5) *Denial-of-Service Attack:* Such attack prevents normal use of network services by valid users. For example, this can be achieved by flooding the network with fake requests and abnormal traffic which results in loss of access to network services or server overload.
6) *Sniffer Attack:* An attacker may use a sniffer application to capture/read network data packets. If data packets are not encrypted, a sniffer may be able to gain information traversing the network, such as passwords, account information, etc.
7) *Application-Layer Attack:* This kind of attack allows the attacker to bypass normal access controls of a server's operating system or applications. In turn, the attacker may modify network settings, introduce a virus program or even disable other security controls.

The above outlined security attacks entail serious measures to protect sensitive data as well as critical network services. No matter how well a network is protected, there will be an incident which IT professionals or computer security specialists may not be prepared to handle by themselves. This may be due to the problem requiring technical capabilities beyond what is currently available or deployed, or due to a lack of authority to make necessary decisions or take necessary actions. Therefore, no enterprise's security policy is considered complete until all efficient and timely precautionary and reactive procedures have been implemented for handling and recovering from any destructive or damaging incidents. Consequently, government agencies and other organizations have begun to complement their computer security efforts due to increased threats to computer networks and services. This is what motivated this study to investigate and present a computer emergency response team for Kuwait.

A possible solution to computer security-related incidents resides in establishing and implementing a Computer Security Incident Response Capability (CSIRC) within an enterprise, which has incident response and handling procedures. The primary objective of CSIRC is to react quickly and efficiently to computer security incidents, so that computer viruses, unauthorized user activity, and serious software vulnerabilities can be handled and resolved in an efficient and timely manner. In addition, a CSIRC may further promote security-awareness of computer security-related threats and risks, so that agencies become well-prepared and protected (Boyce and Jennings, 2002).

Generally speaking, the terms *incident response* and *incident handling* are used synonymously and interchangeably to describe reactive procedures to prevent disruption of data or system integrity, or denial of service availability. There are several other terms derived from CSIRC,

including CSRC (Computer Security Response Center), CSIRT (Computer Security Incident Response Team), CIRT (Computer Incident Response Team), and CERT (Computer Emergency Response Team). In this thesis, the acronym CERT will be used throughout (Wikipedia, 2014).

1.2 Problem Definition

Cyberspace security and computer security-related awareness on potential threats and corresponding event-handling procedures are of paramount importance in today's businesses and enterprises. Our research focuses on the study of the fundamentals of a CERT, which protects Internet applications and data-sensitive services and processes against security-related incidents, and characterizes the capabilities and limitations of CERT in Kuwait (KW-CERT). Light is shed on several security-related deficiencies in KW-CERT exposed by a survey study, upon which several potential solutions and remedies are proposed. This research also focuses on KW-CERT as a smart practice and focuses on specific components and how they can be connected to different organizations and sectors in Kuwait. Special attention will be given to these points:

A. Security incident management and incident response, and the current best practices.
B. The major security-threats to information systems in Kuwait.
C. The level of security awareness and practices in Kuwait.
D. Improvements of information security incident identification and response in Kuwait.
E. Connecting the different governmental and non-governmental sectors in Kuwait under KW-CERT.
F. Proposing solutions and practices for improving information security incident identification and response in Kuwait.

To ultimately achieve the objective of this thesis, several things must be performed. First, an extensive study of existing literature on CERTs from around the world and their related global organizations is provided. Second, the main components of KW-CERT are thoroughly studied. After that, IT specialists and employees will be asked to take and comment on a survey related to security practices and awareness. The feedback and results obtained from the survey will form an important input to the study. Particularly, the interpretation and analysis will be used as a basis for security management and solution strategies of KW-CERT.

1.3 Significance of Study

The contributions of this study would be of interest to scholars, IT and computer security experts in Kuwait. Particularly, the findings of thesis will provide guidelines on establishing a computer emergence response team in Kuwait by considering the level of security-related awareness, organizing

and responding to cyber-security incidents and activities, investigating and implementing superior cyber-security mitigation and practices, and building a framework of the most up-to-date solutions. Moreover, this study will draw the attention of IT experts and managers to estimate and necessary funding for start-up costs (software, supplies, Internet domain registration fees, facilities costs) and human resources costs (salaries, benefits and specialized training courses). Finally, this study will ensure that KW-CERT will be a solid authoritative element or capability that provides incident response management and handling for governmental and private sectors in Kuwait.

1.4 Overview of CERT

Introduction

Historically, the designation of the computer emergency response team is due to the first team (CERT/CC) at Carnegie Mellon University (CMU). Currently, CERT is a registered service mark of CMU, which is also licensed to other incident response teams in the world. After a worm hit the Internet in Nov. 1988 (known as Morris Worm), a considerable percentage of the Internet was paralyzed. This called for the formation of the CERT/CC at CMU, under a U.S. Government contract (Wikipedia, 2014). There are various types of CERTs. For instance, an internal CERT is assembled as part of a parent organization, such as government, a corporation, a university or a research network. Another type is National CERTs, which oversee incident handling for an entire country.

This Chapter gives an overview of the fundamentals of a CERT along with examples of existing CERTs and international organizations.

1.5 What is a CERT?

A CERT is a group of carefully selected and well-trained individuals who specialize in promptly handling computer security threats, so that it can be quickly contained, investigated and recovered from. Such individuals should have the authority to make decisions and take actions, combating any potentials threats on network services and the Internet.

The main human resources needed to build a CERT are discussed in the following subsections (Wikipedia, 2014) and (SANS Institute, 2001).

1.5.1 Management

The management team should be involved in the whole security process such as evaluating security, hiring the right staff, developing a policy, exercising a plan, making big decisions involving incident assessment and responses (Wikipedia, 2014).

1.5.2 Information Security

The members of the Information Security team are essential components of a CERT as they are specialists in handling a multitude of incidents, and providing options and implications of these options to managements and other teams. They can also assess the extent of the damage, containment, basic forensics and recovery.

1.5.3 Information Technology (IT)

The responsibility of the IT team is to care for the important data and how it can be accessed and backed-up. In addition, the IT members should work hand in hand with the Information Security team on any technical matters required.

1.5.4 IT Auditor

The role of IT auditors is to ensure that all policies and procedures are thoroughly followed. In addition, they observe, learn why an incident happened, ensure that all procedures are closed followed and conduct post-incident reviews.

1.5.5 Security

The security team is the one responsible for implementing physical security systems. In addition, they should be able to assess any physical damage, investigate physical evidence, and guard evidence during a forensics investigation to maintain a chain of evidence.

1.5.6 Attorney

An attorney is needed to provide a CERT with legal advice. This is specifically important when collecting evidence during an investigation, with the possibility of taking a legal action. An attorney can also provide advice on liability issues in case a security incident affects customers, vendors, and/or the general public.

1.5.7 Public Relations

Public relations representatives are needed to maintain the image of an enterprise and keep minor incidents away from the media. In case of major incidents, a representative may provide advice on the best way to convey the message to the public and/or stakeholders, with the least damage possible. In addition, their responsibility lies in communicating with team leaders to ensure accurate understanding of the enterprise’s status.

1.5.8 Financial Auditor

When an incident occurs, it is essential to put a monetary figure on the damage caused, as this is required for insurance companies. This is also important in order to press charges after completing all related security forensics and investigations.

In addition to these members, other professionals might be needed, such as law enforcement, vendors, and/or technical specialists.

1.6 What is Needed to Implement a CERT?

It is essential to appreciate the process of planning to create a successful CERT. Basically; this process starts by writing proper incident response procedures under management supervision. Without their support, the CERT is not assured adequate funding or authority. Moreover, it might be necessary to outsource professionals to build a security system, without which, the process cannot progress. Consequently, security procedures must be carefully developed based on the available resources made by the management (SANS Institute, 2001).

After that, one must establish what exactly constitutes an incident and at what point the team should be called in. Specifically, it must be noted that calling the CERT too frequently over minor issues might slow down reaction time. Contrarily, one must not underutilize the team. Striking a balance and documenting when to utilize a CERT as clearly as possible is essential. The process of calling a team must be done through a team leader and contact person. After assessing the situation and severity of the incident, the leader may contact the required team members. Generally speaking, it is preferred to contact as few people as possible during the initial containment period. Additionally, a list of names and methods for contacting specific members during on-work and off-work hours should be made available to all members of the team. Specifically, there should be at least one non-email way of contact.

As soon as the incident response, incident handling and incident follow-up procedures have been documented, an initial meeting with the CERT members should be held. Every team member must fully understand and appreciate his/her role in the team, and the need to respond quickly when called upon. They should also understand the kind of situations they may face and the urgency in responding and working with the other team members. This in turn requires intensive training to all team members with several drills scheduled. Procedures must be documented during the practice incidents and a post-incident review meeting must take place to go over all incident-related issues and practices. This practice serves two main purposes. The first is to prepare the team members so that they can better understand their roles and duties within the team. The second purpose is to discover any procedural holes. After that, it is important to meet and review

the exercise. It is also important to conduct a practice exercise often and then review the enterprise's incident response procedures.

1.7 Existing CERTs

All CERTS (or equivalently CIRTs) are different. Each organization must decide on the structure and operation that works for it. This is because solutions that work for one organization may not work for another, due to various constraints and region-specific regulations and situations. All across the globe, there are many professional groups of experts working together to make sure that the Internet and ICT function properly.

In the following subsections, the Australian CERT, Japanese CERT, US CERT, Brazil CERT, Qatar CERT, and UAE CERT are discussed. Other CERTs can be found in (Forum of Incident Response and Security Teams, 2014).

1.7.1 Australian Computer Emergency Response Team (AusCERT)

The Australian CERT (AusCERT) operates within a worldwide network of information security experts, and hence provides information security advice to the Australian public, its members, including the higher education sector, making it a leading CERT in the Asia/Pacific region. The AusCERT is non-profit self-funded organization that is based at the University of Queensland (Australia Computer Emergency Response Team, 2010). It was formed in 1993, thus is considered one of the oldest CERTs in the world, and was the first CERT in Australia to operate as the national CERT until 2010, when it was replaced by CERT Australia (i.e. the national CERT of Australia). CERT Australia works closely with the Australian Federal Police (AFP), and the Australian Signals Directorate (ASD) (Australian Government – CERT Australia, 2015).

AusCERT provides preventive services against global computer network threats and vulnerabilities in a time critical manner. In addition, AusCERT publishes security bulletins, which contain latest prevention and mitigation techniques, as well as practical advice on incident management. AusCERT is an active member of FIRST, the global Forum of Incident Response and Security Teams, and the Asia-Pacific CERT (AP-CERT).

1.7.2 Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) is the first CSIRT to be established in Japan. Globally, it is a member of FIRST and it acts as a secretariat for AP-CERT. In 1992, JPCERT began its activity as a Security Task of JEPG/IP[1] by a

[1] JEPG/IP stands for Japan Engineering and Planning Group on IP.

group of volunteers. In Oct. 1996, the JPCERT/CC was officially established. In Aug. 1998, the JPCERT/CC joined FIRST; while in Feb. 2003, it helped establish the AP-CERT and was then appointed as a Secretariat of AP-CERT. In Mar. 2003, it was registered publicly and obtained its legal status, becoming an independent non-profit organization (Japan Computer Emergency Response Team Coordination Center, 2003).

The objectives of JPCERT/CC include coordinating with domestic and international CSIRTs and fostering the establishment of a new CSIRT and collaboration among CSIRTs. It also aims at gathering and disseminating technical information on computer security incidents and vulnerabilities and security fixes. Other objectives and activities are given in Figure 1-3.



Figure 1-3
JPCERT/CC Activities (Source: About JPCERT/CC , 2003)

1.7.3 United States Computer Emergency Readiness Team (US-CERT)

The United States Computer Emergency Readiness Team (US-CERT) is part of the US Department of Homeland Security (DHS) – National Protection and Programs Directorate. US-CERT was established in Sept. 2003 to protect the Internet infrastructure of the U.S. in response to cyber-attacks (United States Computer Emergency Readiness Team, 2002). It is operational on a 24 hours/7 days a week basis, providing technical assistance to information system operations and disseminating timely notifications regarding current and potential security threats and vulnerabilities. US-CERT partners with private sector critical infrastructure owners and operators, academia, federal agencies, and domestic and international organizations to enhance the Nation's cyber security posture. In addition, it strives for a safer, stronger Internet by responding to major incidents, analyzing threats, and exchanging critical cyber security information with trusted partners around the world. In Nov. 2012, US-CERT merged with the DHS' National Cyber security and Communications Integration Center (NCCIC). Now, the US-CERT consists

of the following branches (IT Law Wikia. United States Computer Emergency Readiness Team):

1. *Operations:* its main role is to receive and response to incidents, disseminate cyber security information and analyze various types of data in response to critical cyber-threats.
2. *Situational Awareness:* this branch is responsible for identifying, analyzing and comprehending broad network activity.
3. *Future Operations:* established in Jan. 2007 to participate in the development of related policies, protocols and procedures in response to cyber-attacks.
4. *Mission Report:* this branch manages US-CERT's communications mechanisms, such as reports, alerts, and notices.

1.7.4 Computer Emergency Response Team Brazil (CERT.br)

The Brazilian National Computer Emergency Response Team (CERT.br) is responsible for handling computer security incident reports and activities related to networks connected to the Brazilian Internet. CERT.br is maintained by NIC.br, the executive branch of the Brazilian Internet Steering Committee. In addition to incident handling and support, CERT.br also participates in increasing security awareness in the Brazilian community. The CERT.br was established in 1997 by the Presidential Decree No. 4829 to establish strategic directives related to the use and development of the Internet in Brazil (Brazilian National Computer Emergency Response Team, 2014). In addition, it is involved in studied and recommends procedures, rules and technical and operation standards for the security of network services as well as the Internet.

The CSIRTs in Brazil can be summarized as in Table 1-1.

Table 1-1
CSIRTS in Brazil
(Brazilian National Computer Emergency Response Team, 2014)

Sector	**CSIRTs**
National Responsibility	CERT.br
Government Networks	CTIR Gov, GATI, GRA/SERPRO
Financial Sector	CSIRTBB, CSIRT Banco Real, CSIRT Santander, Visanet CSIRT
Telecom/ISP	Brasil Telecom, CTBC Telecom, EMBRATEL, CSIRT Telefonica
Academic and Research Networks	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CSIRT USP
Outsourcing	CSIRT TIVIT

1.7.5 Qatar Computer Emergency Response Team (Q-CERT)

Q-CERT is the national computer information security team of the State of Qatar, and it was established in December 2005. Specifically, Q-CERT was established as a project of the Supreme Council for Information and Communications Technology (ictQATAR, 2005). Q-CERT aims at identifying their most important information assets and developing risk management strategies. In addition, it works on recognizing cyber-attacks and responding effectively. Moreover, Q-CERT works with other security teams around the world to maintain awareness of global trends and coordinate response to international threats and incidents. Also, Q-CERT offers tailored workshops based on needs analysis and also public workshops based on recognized needs (Q-CERT, 2007).

Q-CERT has actively participated in the establishment of the regional Gulf Cooperation Council CERT (GCC-CERT), in its efforts to respond to incidents within Qatar and the region (more later). Q-CERT is also a member of FIRST (The Report: Emerging Qatar, 2007).

1.7.6 United Arab Emirates Computer Emergency Response Team (aeCERT)

In June 2008, the United Arab Emirates (UAE) Cabinet of Services has approved the UAE CERT (aeCERT) as the National CERT for the UAE by decree number 89/2005. Effectively, aeCERT was initiated by the Telecommunications Regulatory Authority (TRA) of the UAE. In addition, the aeCERT has been enlisted with the CERT/Coordination Center of the United States, granting it the official acknowledgement worldwide as the UAE National CERT (United Arab Emirates – Computer Emergency Response Team, 2015). In July 2008, the aeCERT launched its operations to facilitate the detection, prevention, and response of security incidents on the Internet. The aeCERT acts an advisory and not as a regulatory body, recommending the implementation of best practice policies, standards, procedures, guidelines and technologies to constituents. It will also serve the UAE government, law enforcement, and business sectors.

The aeCERT missions include sustaining a resilient and vigilant ICT infrastructure against security threats, and building a secure and safe cyber culture across the UAE (Telecommunications Regulatory Authority of the UAE, 2009). In addition, the aeCERT aims at enhancing security awareness in the UAE as well as providing a central trusted point of contact for cyber security incident reporting in the UAE. In addition, fostering the establishment of and providing support to sector-based CSIRTs, along with coordinating with domestic and international CSIRTs.

In its efforts to build and promote a safer cyber culture within the UAE and across the GCC, aeCERT held the first UAE and GCC National Security Awareness campaign in Nov. 2007 (Telecommunications

Regulatory Authority of the UAE, 2009). The aim of such campaign was to raise awareness and educate people on the key security issues facing businesses, individuals, students, and children. Particularly, the campaign provided the public with e-Learning modules, focusing on protecting information and online identity as well as the essentials of Internet threats and cyber security. In 2009, the Security Awareness Assessment program was established to assess the security awareness level across different sectors within the UAE.

1.8 International Organizations

Several organizational entities have been established to coordinate and monitor the Internet in collaboration with the regional network service providers, security vendors, government agencies as well as industry associations. Such organizations can provide services and support to participating CSIRTs. More importantly, they allow different CERTs to share similar legislative and cultural issues to collaborate and coordinate incident handling activities. In addition, a regional CSIRT organization can assist with analysis and resolution of incidents and vulnerabilities. Moreover, it promotes common standards and procedures for coordination, and the following are examples of such organizations.

1.8.1 Forum of Incident Response and Security Teams (FIRST)

FIRST, established in 1990, is a coalition of CSIRTs, bringing together a variety of computer security incident response teams from government, commercial and academic organizations (Forum of Incident Response and Security Teams, 2014). FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large. Currently, there are 295 teams across 64 countries working with FIRST (Figure 1-4). FIRST is considered the global association of CSIRTs.

FIRST offers two types of memberships[2]:

A. *Full Members:* This type of membership pertains to organizations that assist in information technology community or other defined constituency in preventing and handling computer security-related incidents.
B. *Liaison Member:* these are individuals or representatives of organizations other than CERT or security teams, which share common interests with FIRST.

[2] The lists of full and liaison members of FIRST can be found in [12].



Figure 1-4
Members of FIRST
(Forum of Incident Response and Security Teams, 2014)

1.8.2 Collaboration of Security Incident Response Teams in Europe (TF-CSIRT)

The TF-CSIRT, promoted by TERENA – Trans-European Research and Education Networking Association, is a European Task Force that is responsible for encouraging collaboration and coordination between CSIRTs in Europe as well as neighboring regions (Trans-European Research and Education Networking Association, 2014). Additionally, it is responsible for liaising with other global organizations. Moreover, TF-CSIRT creates a forum where members of CSIRT community can exchange experiences, knowledge and solutions, and also to certify service standards. Furthermore, it coordinates joint initiatives, including training of staff and assisting in the establishment of development of new CSIRTs. Also, it collaborates with FIRST, the European Union Agency for Network and Information Security (ENISA) (European Union Agency for Network and Information Security, 2005), and other regional CSIRT organizations as well as law enforcement agencies. A few member CSIRTs of the TF-CSIRTs are summarized in Table 1-2. For a more comprehensive list of CSIRTs, the reader is referred to (TF-CSIRT Trusted Introducer, 2014).

Table 1-2
List of TF-CSIRT Members (TF-CSIRT Trusted Introducer, 2014)

Country	CSIRT/CERT	Country	CSIRT/CERT
Albania	ALCIRT	Iceland	CERT-IS
Armenia	CERT AM	Ireland	IRISS CERT
Austria	R-IT CERT	Italy	PI-CERT
Belgium	BELNET CERT	Netherland	AMC-CERT
Bulgaria	CERT Bulgaria	Norway	NorCERT
Croatia	CERT ZSIS	Poland	CERT POLSKA
Czech Republic	CESNET-CERTS	Portugal	CERT.PT
Denmark	Danish GovCERT	Romania	CERT-RO
Estonia	CERT-EE	Spain	AndaluciaCERT
Finland	Funet CERT	Sweden	CERT-SE
France	CERT-FR	Switzerland	BVCERT
Germany	Deutsche Telekom CERT	Ukraine	CERT-UA
Greece	GRNET-CERT	United Kingdom	CSIRTUK
Hungary	CERT-Hungary		

1.8.3 Asia-Pacific Computer Emergency Response Team (AP-CERT)

The Asia-Pacific CERT (AP-CERT) cooperates with CERTs and CSIRTs to ensure Internet security in the Asia-Pacific region, and to promote information sharing, and trust (Asia-Pacific Computer Emergency Response Team, 2014). Specifically, it encourages collaboration to clean-up infected systems and networks, and provide reliable communications and information sharing. Also, it maintains a trusted network of security experts to improve the region's security awareness. Moreover, AP-CERT collaborates with other CERTs and CSIRTs for effective research and development on computer emergency response and provides recommendations on legal issues related to information security and network security incidents. Originally AP-CERT was known as APSIRC, which stands for Asia-Pacific Security Incident Response Coordination. The name was changed to AP-CERT in Feb. 2003.

There are two types of members under the umbrella of AP-CERT (Asia-Pacific Computer Emergency Response Team, 2014):

A. *Operational Member:* is a member of the Asia-Pacific region that operates in full-time basis as a leading or national CSIRT/CERT, within its own economy.
B. *Supporting Member:* is a security-related entity, which may not necessarily be in the Asia-Pacific region but can support and contribute to AP-CERT operations and CSIRT/CERT functions.

Table 1-3 summarizes the members of AP-CERT.

Table 1-3
List of Operational and Supporting Members of AP-CERT
(Asia-Pacific Computer Emergency Response Team, 2014)

Member Type	Country	CERT
Operational	Australia	AusCERT
	Bangladesh	bdCERT
	China	CCERT
	Hong Kong	HKCERT
	India	CERT-In
	Indonesia	ID-CERT
	Japan	JPCERT/CC
	Korea	KrCERT/CC
	Malaysia	MyCERT
	New Zealand	NCSC
	Singapore	SingCERT
	Taiwan	EC-CERT
	Thailand	ThaiCERT
	Vietnam	VNCERT
Supporting	Bkav Corporation	
	Microsoft Corporation	

1.8.4 Gulf Cooperation Council Computer Emergency Response Teams (GCC-CERT)

The concept paper on regional GCC-CERT was first proposed in April 2006. After several workshops and meetings, the GCC-CERT was formally established in May 2008 by decision of the Gulf Cooperation Council, as collaboration amongst the emerging GCC national programs (Lewis, 2008). The GCC decision established a framework for regional cooperation amongst Gulf States (Oman, UAE, Qatar, Kuwait, Saudi Arabia, and Bahrain) on the topic of information security. Furthermore, several GCC countries are developing "cyber authorities" at the national level to combat online adversaries and protect critical national infrastructure.

Working group meetings are ongoing to fulfill the GCC instructions to share views, best practices, given recommendations on the issues related to the cyber security. For instance, over 20 workshops and group sessions were offered in the GCC countries in the first year of operation. Currently, the CERT of the State of Qatar (Q-CERT) is leading the development of the GCC-CERT, which takes under its wing the CERTs listed in Table 1-4. It should be noted that the CERTs of Kuwait (KW-CERT) and Bahrain (B-CERT) have not been fully established and they are currently under development.

Table 1-4
List of GCC CERTs
(Lewis, 2008)

Country	**CERT**
Qatar	Q-CERT
UAE	aeCERT
KSA	CERT-SA
Oman	OCERT
Bahrain	B-CERT
Kuwait	KW-CERT

1.8.5 Organization of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT)

The Organization of the Islamic Cooperation CERT (OIC-CERT) was established in June 2008 based on Resolution No. 3/35-INF, during the 35th Session of the Council of Foreign Ministers of the OIC meeting in Kampala, Uganda. The formation of CERT among OIC member countries was first proposed during the Annual Meeting of Islamic Development Back Board of Governors at Putrajaya, Malaysia, in June 2005 (The Organization of the Islamic Cooperation – Computer Emergency Response Team, 2014). In July 2006, the first OIC-CERT Task Force Meeting was held in Kuala Lumpur, Malaysia (Cyber Security Malaysia), with Tunisia (National Agency for Computer Security) being appointed as the Chairman and Secretariat.

The OIC-CERT aims at providing a platform for member countries to explore and to develop collaborative initiatives and possible partnerships in matters pertaining to cyber security that shall strengthen their self-reliance in the cyberspace. In addition, it encourages experience and information sharing in the ICT security. Moreover, the OIC-CERT fosters education and outreach of ICT security programs. Furthermore, it takes part in assisting member countries in establishing National CERTs.

The OIC-CERT is open to any type of CERT that shares similar objectives with it. Additionally, the OIC-CERT has five membership levels (The Organization of the Islamic Cooperation – Computer Emergency Response Team, 2014):

1) *Full Member:* must operate within OIC member country with the power to present country interest. It must also be non-profit based, wholly, or party government funded. In addition, a full member has the right to vote and stand for election to be in the Steering Committee.
2) *General Member:* This type of membership covers private sectors, non-governmental organizations, and Academia. Specifically, any private CERT entity from OIC-CERT country with no authority to present country interest may become a general member.
3) *Professional Member:* Individuals who are experts in information security with the sole purpose to give export advice to security-related matters may become professional members.
4) *Commercial Member:* Industrial or business organizations that deal with cyber security matters fall under commercial members.
5) *Affiliate Member:* This type of membership covers non-profit institutions of Non-OIC-CERT countries as shown in Table 1-5 lists the member organizations of the OIC-CERT.

Table 1-5
List of Member Organizations of OIC-CERT
(The Organization of the Islamic Cooperation – Computer Emergency Response Team, 2014)

Membership Type	Member
Steering Committee	1. Information Technology Authority (Oman) 2. National Agency for Computer Security (Tunisia) 3. CyberSecurity Malaysia (Malaysia) 4. Consultancy Support Services Limited (Nigeria) 5. Ministry of Communication and Information Technology (Egypt) 6. Indonesia Security Incident Response Team on Internet Infrastructure (id-SIRTII) (Indonesia) 7. Computer Emergency Response Team (aeCERT) (UAE)
Full	1. Moroccan National Computer Emergency Response Team (maCERT) 2. Information Technology Authority (Oman) 3. National Agency for Computer Security (Tunisia) 4. CyberSecurity Malaysia (Malaysia) 5. National Agency for Network Services (Syria) 6. National Response Center for Cyber Crimes (Pakistan) 7. Consultancy Support Services Limited (Nigeria) 8. National Center for Security and Crisis Management (NCSCM) (Jordan) 9. Iran CERT (IrCERT) (Iran) 10. Brunei Computer Emergency Response Team (BRUCERT) (Brunei) 11. Computer Emergency Response Team – Saudi Arabia (CERT-SA) (Saudi Arabia) 12. Ministry of Communication and Information Technology (Egypt) 13. Indonesia Security Incident Response Team on Internet Infrastructure (id-SIRTII) (Indonesia) 14. National Information Security and Safety Authority (NISSA) (Lybia) 15. Computer Emergency Response Team (aeCERT) (UAE) 16. Sudan Computer Emergency Response Team (sudanCERT) (Sudan) 17. Azerbaijan Government CERT (CERT.GOV.AZ) (Azerbaijan)
General	18. The Awareness, Prevention and Assistance Professional CERT Center – Isfahan University of Technology CERT (APA-IUTcert) (Iran) 19. The Awareness, Prevention and Assistance Professional CERT Center – Amirkabir University of Technology CERT (APA-AUTcert) (Iran) 20. APA – Sharif University (APA – SharifCERT) (Iran) 21. APA – Shiraz University (APA – SUcert) (Iran)
Honorary	1. Organization of Islamic Cooperation (Saudi Arabia)
Commercial	2. Telekom Applied Business SDN BHD (Malaysia)

1.9 Summary

In this Chapter, an overview of CERTs has been given. In addition, examples of existing CERTs from around the world have been presented. Moreover, several regional and international organizations supporting CERTs have been outlined.

Chapter 2

KW-CERT Framework

2.1 Introduction

The Central Agency for Information Technology (CAIT) plans to establish a National Computer Emergency Response Team for the State of Kuwait (i.e. KW-CERT) that is responsible for the protection of governmental and non-governmental administrative networks and national IT resources connected to the Cyberspace[3] (The Central Agency for Information Technology, 2006). It will act as a national point of contact (PoC) for information sharing (like incident reports, vulnerability information and others) with other national CERTs existing worldwide.

KW-CERT is expected to have incident management capability in place with comprehensive set of processes for handling computer security incidents covering response, management, and coordination processes for such incidents. The following mission statement has been derived from CAIT's mandate, experience and knowledge of the IT security status in the government sector (Control and Protection of National Information Technology Infrastructure, 2011):

"Developing a national team of educated, trained, knowledgeable, and aware practitioners who understand the risks and issues related to cyber-security incidents and the threats and attacks from vulnerabilities; capable to respond to computer security incidents, support their constituents to recover from computer security breaches and provide them with preventative and educational services."

This Chapter outlines that KW-CERT framework, its services and policies, procedures and team’s operations. Finally, this Chapter concludes with the role of an international consultant for effective deployment of KW-CERT.

2.2 KW-CERT Constituency

The KW-CERT is expected to be the umbrella team for the security of information technologies in the State of Kuwait. It should be able to facilitate and coordinate activities among a diversity of agencies (government, academic, critical resources and infrastructures, private, etc.), to share information and address computer security problems. It should also develop mechanisms for trusted communications with and within these agencies. An essential task for the KW-CERT is to define its constituency and its relationship to that constituency, and then promote regional and international cooperation on related information and knowledge sharing.

---

[3] CAIT is a government organization established according to the terms of Article (2) of the Amiri Decree No. (266/2006).

KW-CERT’s constituency should be addressed based on the components discussed in the following subsections(Control and Protection of National Information Technology Infrastructure, 2011; Schultzand Shumway, 2001).

2.2.1 KW-CERT Constituency Relationship

As mentioned above, KW-CERT will deal with diverse agencies. Depending on the range of services offered by KW-CERT and the nature of those services, KW-CERT needs to define each constituency. Generally speaking, the constituency of a CERT refers to the customer base for its services. So, in theory, the constituency of KW-CERT consists of all entities with the state’s borders. This is due to the fact that any domestic entity is a potential customer of the national/governmental CERT. Moreover, the constituency of a national/governmental CERT can typically be broken down into subgroups, according to the services CERT delivers to the entities in the group, or based on the responsibilities the CERT carriers with regards to the group. Thus, these multiple subgroups/agencies might intersect, be sub- or supersets, overlap or be totally separate from other agencies served by KW-CERT. Typically, the following constituency subgroups can be distinguished:

I. *Government and Public Bodies:* KW-CERT will provide its full range of services to the government and public bodies.
II. *Critical Information Infrastructure (CII) Organizations:* KW-CERT may provide its full range of services to CII organizations. However, in most cases, private CII organizations have IT or information security personnel responsible for handling security incidents. In such cases, KW-CERT may play a more coordinating or supporting role.
III. *Other Stakeholders with the State’s Borders:* KW-CERT will provide a subset of its services to any other domestic stakeholders or the broad public interest.

It is noteworthy that other groups of constituents may be distinguished as well. For instance, research and education networks/institutions will remain a special group of constituents for KW-CERT.

The nature of the relationship between a KW-CERT and its constituency will directly affect the nature of the services that the KW-CERT offers. The relationship with any agency may imply some constraints that should be addressed too. Moreover, such relationship will fall into three categories (or levels of authority), as follows.

1) *Full Authority:* Members of the KW-CERT have the authority to undertake any necessary actions or decisions on behalf of their constituency.

2) *Shared Authority:* Members of the KW-CERT provide direct support to their constituents and share in the decision-making process (i.e. have influence on decisions, but are unable to dictate to them).
3) *None:* Members of the KW-CERT have no authority over their constituency and can act only as advocates or advisors.

2.2.2 Promoting KW-CERT to Constituency and Gaining Trust

It will be important to publicly advertise and clearly outline the constituency definition and the KW-CERT services to ensure that both the constituency and other parties understand what interactions they might expect with KW-CERT. KW-CERT should be able to promote itself and its services as widely as possible to ensure that its declared constituency is aware of the team, ensure that other teams know of the KW-CERT and the constituency it serves, and to gain broader recognition of the team in general. This is expected to be achieved through many communication channels, including:

A. Constituency email lists and newsgroups.
B. KW-CERT or organizational information/web server.
C. Presentation, workshop, and tutorial materials.
D. General awareness materials, newsletters and media.

KW-CERT cannot operate effectively without gaining and maintaining the constituency's trust and confidence even if it has full authority over its constituency. This trust must be earned and nurtured. As KW-CERT gains the trust and respect of its declared constituency, more of the declared constituency will begin to recognize and support the team, resulting in the growth of the team's reporting constituency.

2.2.3 Place in the Organization

KW-CERT will be part of the organizational structure of CAIT (the parent organization); specifically, as a supervision unit under the Division of Technology and Infrastructure. The place of the KW-CERT should be in line with its mission statement. It is regarded that the main task of the national CERT is incident handling; therefore, the relation with the organizational team as well as other security teams in other organizations should be structured and organized. Furthermore, it is important to address the role of KW-CERT with relation to security risk analysis in the context of organizational risk as well as technical risk.

2.2.4 Relationship to other Teams

IT is crucial for KW-CERT to integrate into the relevant CERT communities (e.g. FIRST, TF-CSIRT, AP-CERT, GCC-CERT, etc.). This is important for its personal knowledge, reputation and information sharing, which are all considered to be part of the criteria for building trust and

successful cooperation on national and international levels. Only with a good functioning cooperation on national level, a national/governmental CERT can fulfill its role on international level, where it is considered as the national PoC for information sharing. Moreover, building a community of key players for network information security and critical information infrastructure protection on national level should be a paramount goal for each national/governmental CERT.

2.2.5 Services and Quality Framework

Based on best practices, the mission statement of KW-CERT will essentially have three derivatives—services, policies, and quality—each of which needs to embody the scope and purpose of the mission statement. The services offered by a team are the methods used to carry out the team's mission. Services are usually provided to the team's constituency. Policies are the governing principles under which the team operates. Quality is the desired standard at which all activities will be undertaken. The information flowing within a KW-CERT permeates all of the mission statement derivatives. Governed by services, policies, and quality, procedures specify how activities are enacted. This framework is depicted in Figure 2-1. The services that will be provided by KW-CERT to its constituents will be based on this framework (Control and Protection of National Information Technology Infrastructure, 2011).

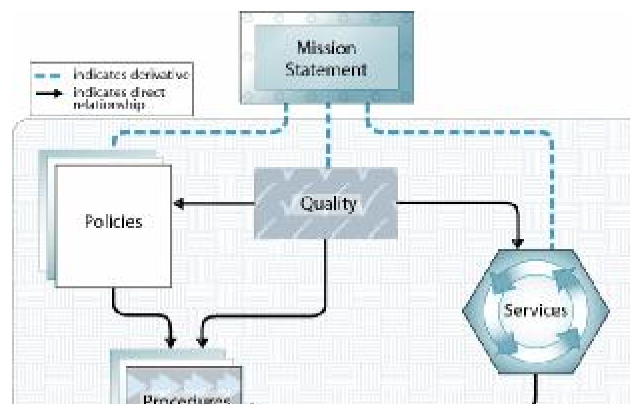


Figure 2-1:
Service and Quality Framework (**Schultz and Shumway, 2001)**

2.3 KW-CERT Services

The services that will be provided by KW-CERT can be grouped into three categories, as discussed in the following subsections.

2.3.1 Reactive Service

These services are triggered by an event or request such as a report of a compromised host or a wide-spreading malicious code. Reactive

services are the core component of KW-CERT operation. Services under this category include (West-Brown, Stikvoort, Kossokowski, Killcrece, G., Ruefle and Zajicek, 2003; ENISA, 2015:

2.3.1.1 Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem.

2.3.1.2 Incident Handling

Incident handling involves receiving, triaging and responding to requests and reports, and analyzing incidents and events. This service is further categorized based on the type of activities performed and the type of assistance given as follows.

2.3.1.3 Incident Analysis

Incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. Two subservices may be done part of incident analysis (and this may include coordination with related governmental entities):

A. *Forensic evidence collection:* the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise.
B. *Tracking or tracing:* the tracing of the origins of an intruder or identifying systems to which the intruder had access.

2.3.1.4 Incident Response on Site

The KW-CERT provides direct, on-site assistance to help constituents recover from an incident. The KW-CERT itself physically analyzes the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (as explained below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs.

2.3.1.5 Incident Response Support

The KW-CERT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve technical assistance in the interpretation of data collected,

providing contact information, or relaying guidance on mitigation and recovery strategies.

2.3.1.6 Incident Response Coordination

The KW-CERT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim.

2.3.1.7 Vulnerability Handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities; analyzing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities. This service is further categorized based on the type of activities performed and the type of assistance given as follows.

A. Vulnerability Analysis

   The KW-CERT performs technical analysis and examination of vulnerabilities in hardware or software.

B. Vulnerability Response

   This service involves determining the appropriate response to mitigate or repair vulnerability.

C. Vulnerability Response Coordination

   The KW-CERT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The KW-CERT verifies that the vulnerability response strategy has been successfully implemented.

2.3.1.8 Artifact Handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures.

A. *Artifact Analysis*

   The KW-CERT performs a technical examination and analysis of any artifact found on a system.

B. *Artifact Response*

   This service involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed.

C. *Artifact Response Coordination*

This service involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, vendors, and other security experts.

2.3.2 Proactive Services

These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.

Services under this category include those discussed in the following subsections (Kruidhof, 2014; ENISA, 2013).

2.3.2.1 Announcements

This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium to long-term impact, such as newly found vulnerabilities or intruder tools.

2.3.2.2 Technology Watch

The KW-CERT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. The outcome of this service might be some type of announcement, guidelines, or recommendations focused at more medium-to-long term security issues.

2.3.2.3 Security Audits or Assessments

This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by industry standards. This includes infrastructure review, best practices review, scanning (using vulnerability or virus scanners to determine which systems and networks are vulnerable), and penetration testing (testing the security of a site by purposefully attacking its systems and networks).

2.3.2.4 Configuration and Maintenance of Security Tools, Applications, Infrastructures and Services

This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the KW-CERT constituency or the KW-CERT itself. The KW-CERT may even provide these services as part of their main function.

2.3.2.5 Development of Security Tools

This service includes the development of any new, constituent-specific tools that are required or desired by the constituency or by the KW-CERT itself.

2.3.2.6 Intrusion Detection Services

This service reviews existing IDS logs, analyzes and initiates a response for any events that meet their defined threshold, or forwards any alerts according to a pre-defined service level agreement or escalation strategy.

2.3.2.7 Security-Related Information Dissemination

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include (ENISA, 2013) and (Killcrece and Ruefle, 2008):

1. Reporting guidelines and contact information for the KW-CERT.
2. Archives of alerts, warnings, and other announcements.
3. Documentation about current best practices, and general computer security guidance.
4. Policies, procedures, and checklists.
5. Current statistics, trends in incident reporting, and other information that can improve overall security practices.

2.3.3 Security Quality Management Services

These services augment existing and well-established services that are independent of incident handling, and traditionally performed by other areas of an organization, such as the IT, audit or training departments. Services that fall into this category are not unique to incident handling or KW-CERT in particular. By leveraging the experiences gained in providing the reactive and proactive services described above, KW-CERT can bring unique perspectives to these quality management services that might not otherwise be available. These may include the ones discussed in the following subsections (Killcrece and Ruefle, 2008) and (Internet Governance Forum, 2014).

2.3.3.1 Risk Analysis

Performing this service would conduct or assist with information security risk analysis activities for new systems and business processes or evaluate threats and attacks against constituent assets and systems.

2.3.3.2 Business Continuity and Disaster Recovery Planning

To perform this service, KW-CERTs must involve business continuity and disaster recovery planning for events related to computer security threats and attacks.

2.3.3.3 Security Consulting

KW-CERT can be used to provide advice and guidance on the best security practices to implement for constituents' business operations.

2.3.3.4 Awareness Building

KW-CERT may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks.

2.3.3.5 Education/Training

This might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents. It might be conducted through seminars, workshops, courses, and tutorials.

2.3.3.6 Product Evaluation/Certification

KW-CERT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable KW-CERT or organizational security practices. This service can be provided as an evaluation or through a certification program, depending on the standards that are applied by the organization or by the KW-CERT.

2.4 KW-CERT Policies

Policies are governing principles adopted by organizations or teams. It is important to understand whether they are implementable, enforceable, and function as expected. There are general policies (Fundamental Policies) that are fundamental requirements for any CERT. Moreover, there are overall policies encompassing the services of a CERT; while there are service-specific policies (ENISA, 2012).

The policies need to be clearly stated and understood by all members of the organization. Without that it will not be possible for the staff to correctly implement and enact their responsibilities. Policies for delivering the service are mainly internal guidelines for the team that dictate appropriate behaviors for some specific activity (ENISA, 2012).

It is essential to stress that a policy should not be defined as a set of detailed procedures. A policy should outline essential characteristics for a specific topic area in such a way that all the necessary information is provided on which detailed procedures can be based to help implement the policy, such as those discussed in the following subsections (ENISA, 2012).

2.4.1 Policy Content

The content of a policy is mainly a definition of behavior in a certain topic area. The policy content features are boundary conditions for any policy definition.

2.4.2 Validation

After a policy has been defined it is important to check its validity in practice before actually implementing and enforcing it. Checking validity means finding out if all the ideas in the policy can actually be translated into real-life behavior.

When validating the policies of KW-CERT, it should take into account the following issues (ENISA, 2012):

1) Ensure that the people responsible for the policy validation are not the same people who created the policy.
2) Validate the policy attributes and content features detailed to ensure that policies are not ambiguous.
3) Undertake consistency checking of the policy in relation to other policies, services, and procedures; and also within the policy itself.
4) Validate implement ability and enforceability.

2.5 Procedures

Procedures detail how a team enacts activities within the boundaries of its policies. Procedures can be very beneficial to help make a policy successful. It is important to understand this relationship between policies and procedures and link them together. Corresponding procedures help many staff members stay within the policy guidelines, especially in situations of stress.

For incident handling, it is expected that procedures will be detailed in terms of the following processes (Control and Protection of National Information Technology Infrastructure, 2011) and (FCC, 2001):

1) *Detecting and Reporting:* Ability to receive and review event information, incident reports, and alerts.
2) *Triage:* Actions taken to categorize, prioritize, and assign events and incidents.
3) *Analysis:* Attempt to determine what has happened, what impact, threat, or damage has resulted, and what recovery or mitigation steps

should be followed. This can include characterizing new threats that may impact the infrastructure.

4) *Incident Response:* Actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to prevent the incident from happening again.

For other services we expect that procedures will be detailed in terms of the following functions and their sub-processes, as follows (Control and Protection of National Information Technology Infrastructure, 2011) and (FCC, 2001):

1)Prepare/Sustain/Improve (Prepare):

1. Plan and implement an initial incident management or CSIRT capability.
2. Sustain that capability.
3. Improve an existing capability through lessons learned and evaluation and assessment activities.
4. Perform a postmortem review of incident management actions when necessary.
5. Pass off infrastructure process improvements from the postmortem to the Protect process.

2) Protect Infrastructure (Protect):

1. Implement changes to the computing infrastructure to stop or mitigate an ongoing incident or to stop or mitigate the potential exploitation of vulnerability in the hardware or software infrastructure.
2. Implement infrastructure protection improvements resulting from postmortem reviews or other process improvement mechanisms.
3. Evaluate the computing infrastructure by performing such tasks as proactive scanning and network monitoring, and by performing security and risk evaluations.
4. Pass off to the Detect process any information about ongoing incidents, discovered.
5. Vulnerabilities or other security-related events that were uncovered during the evaluation.

3)Detect Events (Detect):

1. Notice events and report those events.
2. Proactively monitor indicators such as network monitoring, IDS, or technology watch functions.
3. Analyze the indicators being monitored (to determine any notable activity that might suggest malicious behavior or identify risk and threats to the enterprise infrastructure).
4. Forward any suspicious or notable event information to the Triage process.

5. Reassign events to areas outside of the incident management process if applicable.
6. Close any events that are not forwarded to the triage process.

4)Triage Events (Triage):

1. Categorize and correlate events.
2. Prioritize events.
3. Assign events for handling or response.
4. Pass on relevant data and information to the *Respond* process.
5. Reassign events to areas outside of the incident management process if applicable.
6. Close any events that are not forwarded to the *Respond* process or reassigned to other areas.

5)Response (Respond):

1. Analyze the event, and plan a response strategy.
2. Coordinate and provide technical, management, and legal response, which can involve actions to contain, resolve, or mitigate incidents and actions to repair and recover affected systems.
3. Communicate with external parties.
4. Reassign events to areas outside of the incident management process if applicable.
5. Close response, and pass lessons learned and incident data to the *Prepare* function for use in a postmortem review.

So far, two types of procedures were discussed; one for incident handling, and another one for the rest of the services. Both are expected to be linked based on Figure 2-2.

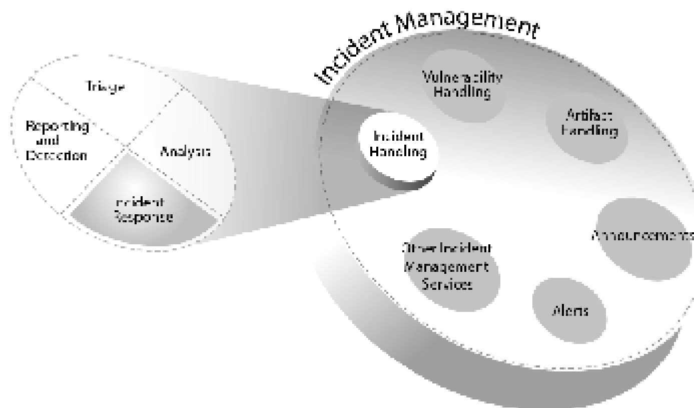


Figure 2-2

Defining the Relationship between Incident Response, Incident Handling, and Incident Management (Control and Protection of National Information Technology Infrastructure, 2011)

2.6 Quality Assurance

IT is required for the work of KW-CERT to be associated with a form of quality assurance which can be sets of quality parameters that backed up

by enforcement and escalation procedures. Based on best practices, a quality system for CERT teams should include (Killcrece and Ruefle, 2008):

1) *Definition of a quality system:* parameters are given that together describe the system's quality.
2) *Checks:* to actually measure these quality parameters
3) *Balances:* To ensure that the results of these measurements are used to assure quality.

2.6.1 Definition of a Quality System

A quality system should be defined using a top-down approach, starting with the mission statement and going down to policies and services, functions that comprise those services, and all associated interactions and procedures. Each element of these will have its own unique subset of quality parameters (Internet Governance Forum, 2014).

2.6.2 Checks

Having defined quality parameters, we also need to define how to check these parameters, how to measure them and how to establish a reporting system. This means that the quality parameters should be validated to be clear, understandable and quantifiable.

2.6.3 Balances

It is important to ensure that staff members are able to accomplish their work to a high standard of quality without overwhelming them with unnecessary hurdles. There is a need to seek the right balance between procedures checking, and the ability to get the job done. Correctly written procedures will ensure a buffer for human errors.

2.7 Team Operations

This part will address operational elements and four operational issues, which are the building blocks of operations that bear a direct relationship to incident handling services (West-Brown, et al., 2003) and (ENISA, 2015).

2.7.1 Work Schedules

A work schedule must differentiate between normal hours and out-of-hours. It includes such things as work shifts, out-of-hours arrangements, backup, and other arrangements.

2.7.2 Telecommunications

This includes traditional telecommunications like telephone, fax, cellular (mobile), pager and automatic response facilities. They are needed

to ensure that KW-CERT and its members can be reached in accordance with set requirements and that staff members have the tools available to initiate communications to the constituency.

2.7.3 E-Mail

A good email system is needed for CERT operations. It is possible to create an easy-to-use, robust email environment that is compliant with up-to date standards for multimedia and security. It is important to consider the need for an interface between the email environment and other environments to handle the workflow needed for KW-CERT operations.

2.7.4 Workflow Management Tools

Tools that help to manage the workflow and hand-over of ongoing tasks are essential especially in environments where people work in shifts with heavy loads. KW-CERT needs a workflow management software tool that enables it to follow and add to the flow of events (such as incidents, requests, or ongoing analysis).

2.7.5 World Wide Web Information Systems

The World Wide Web (WWW) is ubiquitous and currently the hottest medium in use for retrieving information. Certainly no team could do without it. Web servers and any public information server for a KW-CERT (providing public information) must be implemented in a secure fashion to avoid the information being manipulated by unauthorized parties.

2.7.6 IP Addresses and Domain Name

By separating the CERT internal network from all other networks for security reasons, this will require ownership of IP address space dedicated to the team. The Domain Name Service (DNS) should not list sensitive information such as the type of operating system that a particular host is running or give out a complete list of all internal hosts, because this might reveal information useful for a technical or social attack.

2.7.7 Network and Host Security

An incident handling service's internal computers, network, and the connection(s) to other networks must be securely configured and protected against attacks. This means splitting the internal network into compartments with different functions, with the interface to the outside world through a mature firewall. At least two components should exist: an operational network, where all service tasks are handled and the data used is stored, and a test-bed.

2.8 Role of the International Consultant

For effective deployment of KW-CERT, an international consultant is hired to review and suggest modifications to the mission statement based on the results and outcomes of an assessment study. It is also important that the International Consultant addresses situations where the KW-CERT may have an indirect authority (if it needs to exist) with any of the constituents. It is expected that the International consultant will be addressing this relationship along with measures and steps fulfilling the requirements to join and cooperate with the international CERT communities.

Additionally, the international consultant should (Control and Protection of National Information Technology Infrastructure, 2011):

1. Identify the organizational model, authority, and physical location for the national team, as well as the local protection requirements.
2. Identify the type of (government) approval, leadership, and sponsorship that is needed for the KW-CERT to be successful, and obtaining that support.
3. Define the types of roles and responsibilities for the national KW-CERT (and the specific tasks to be undertaken, by whom, when, and under what conditions, the type of recording/tracking required, etc.).
4. Determine key resources, network and information security, and critical information infrastructure that need to be protected.
5. Develop a standardized set of criteria and consistent terminology for categorizing and defining incident activity and events.
6. Develop KW-CERT Logo.

It is expected from the International Consultant to generate policies for all the mentioned services in Sections 3.4 and 3.5. He is expected also to address the fundamental policies as part of the team operations (Section 3.6). Additionally, it is expected that policies will be revised and once revisions are made they should be retested. Once the validation process is completed, they can be implemented or enforced. Once that is done, the policy will need to be maintained by making regular checks on its behavior in real life. Many of these checks will be equivalent to the validation checks, and new checks may be added by the International Consultant where it is seen necessary.

2.9 Summary

In this Chapter, the framework KW-CERT has been outlined. Specifically, KW-CERT's constituency and its relationship to other teams have been discussed. Moreover, the services provided by KW-CERT have been discussed, along with its policies. Additionally, team operations and work management tools have been addressed. Finally, the role of the international consultant for effective deployment of KW-CERT has been discussed.

Chapter 3

KW-CERT Survey Results and Discussion

3.1 Introduction

The national KW-CERT is considered to be responsible for the protection and security of computer networks and IT resources and services connected to the cyberspace in Kuwait. This chapter presents the results of a survey conducted in Kuwait to inquire about the level of security awareness, services and handling of threats across private and governmental sectors. Specifically, there are 37 questions with five possible answers, covering five different topics:

1) Reactive and proactive services (7 Questions).
2) Cyber-attacks (6 Questions).
3) Obstacles impacting information security (7 Questions)
4) Security awareness (12 Questions).
5) Handling security threats (5 Questions).

The questions of each topic are given in Appendix I. The findings and results of this survey will shed light on the necessary security procedures to be implemented in KW-CERT.

3.2 Characteristics of Study Sample

The survey study is mainly aimed at IT specialists from governmental and non-governmental (private) sectors in Kuwait to gauge opinions and receive feedback on the current security practices and level of awareness.

There have been 36 survey takers, designated according to the following criteria:

1. Occupation (Technical Support, Operational, Management or Other[4]).
2. Sector (Governmental or Private).
3. Qualification (Bachelor (IT), Master (IT), Ph.D. (IT) or other).
4. Years of IT Experience (Less than 5 years, 6 – 15 Years, or More than 15 Years).

The following tables summarize and discuss the characteristics of the survey takers. In Table 3-1, a summary of the collected data pertaining to the occupation of the surveyors is given. Specifically, one can see that people working as Technical support form the majority of the survey takes, with 38.89%. Additionally, one can see that 83.33% of the collected data comes from people who are either involved in Technical Support, Operations or Management. This implies that the collected data is mostly

[4] For instance, advanced certifications and diplomas.

accurate and reflects the views of employees that are involved in IT related jobs.

Table 3-1
Summary of Collected Data per Occupation

Occupation	Frequency	Cumulative Frequency	Percentage (%)	Cumulative Percentage (%)
Technical Support	14	14	38.89	38.89
Operational	7	21	19.44	58.33
Management	9	30	25.00	83.33
Other	6	36	16.67	100

Table 3-2 summarizes the collected data per sector, where one can see that the survey takers from the governmental sector are slightly greater than those from the private sector. This suggests the collected data from this survey is well-represented by both the governmental and private sectors.

Table 3-2
Summary of Collected Data per Sector

Sector	Frequency	Cumulative Frequency	Percentage (%)	Cumulative Percentage (%)
Governmental	21	21	58.33	58.33
Private	15	36	41.67	100

In Table 3-3, the qualifications of the survey takers are summarized. It is clear that most of the surveyors (about 69.44%) hold a Bachelor's degree in an IT-related field. More importantly, 88.89% of the survey takers hold either an undergraduate or post-graduate degree related to IT. This in turn implies that the majority of the surveyees have sufficient knowledge/expertise of IT and possibly related security issues.

Table 3-3
Summary of Collected Data per Qualification

Qualification	Frequency	Cumulative Frequency	Percentage (%)	Cumulative Percentage (%)
Bachelor (IT)	25	25	69.44	69.44
Master (IT)	5	30	13.89	83.33
Ph.D. (IT)	2	32	5.56	88.89
Other	4	36	11.11	100

Finally, Table 3-4 lists the years of IT experience of the surveyees. Particularly, one can see that most of the survey takers have 6 – 15 years of IT experience. In general, the majority of the surveyees (about 86.11%) have 15 years or less of IT experience. Moreover, only 13.89% of the survey takers have more than 15 years of experience. Furthermore, one can straightforwardly verify that about 72.22% of the surveyees have not less

than 6 years or IT experience. Therefore, the collected data can be considered to be reliable.

Table 3-4
Summary of Collected Data per Years of IT Experience

Years of IT Experience	Frequency	Cumulative Frequency	Percentage (%)	Cumulative Percentage (%)
Less than 5 Years	10	10	27.78	27.78
6 – 15 Years	21	31	58.33	86.11
More than 15 Years	5	36	13.89	100

In summary, most of the survey takers have technical experience with respect to information technology with several years of experience, and they roughly equally represent both the governmental and private sectors.

3.3 Description of Survey and Statistical Measures

3.3.1 Description of Survey

As can be seen in Appendix I, there are five possible answers to each question under each topic, and each question is assigned a numerical value (to indicate its goodness), as follows:

A. Strongly Disagree (1).
B. Disagree (2).
C. Neutral (3).
D. Agree (4).
E. Strongly Agree (5).

Now, to measure the quality of the answers, three levels of goodness have been designated, and the range of values and their associated levels have been determined according to the following formula:

$$Level\ of\ Goodness = \frac{Maximum\ Value - Minimum\ Value}{Desired\ Number\ of\ Levels} = 1.333$$

Therefore, the levels have been categorized as given in Table 3-5.

Table 3-5
Designated Levels of Goodness

Range	Level of Goodness
1.00 – 2.33	Low
2.34 – 3.67	Acceptable
3.68 – 5.00	Good

3.3.2 Statistical Measures

The different statistical measures considered in this chapter are outlined in the following subsections.

3.3.2.1 Sample Mean

The sample mean gives an estimate of the population mean and is determined from the collected data. Particularly, the sample mean $\bar{X}$ gives an average of the collected data X and is given by

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n} \tag{1}$$

where n is the number of collected data observations (William and Robert, 2012).

3.3.2.2 Sample Standard Deviation

The standard deviation SD is a measure of the spread of the collected data about the sample mean, and is given by

$$SD = \sqrt{\frac{\sum_{i=1}^{n} (X_i - \bar{X})^2}{n - 1}} \tag{2}$$

3.3.2.3 Standard Error of the Mean

Standard error of the mean (SEM) tells us how accurate our estimate of the mean is likely to be. The SEM can be estimated using the sample size and sample standard deviation of the collected sample of collected data, according to the following formula,

$$SEM = \frac{SD}{\sqrt{n}} \tag{3}$$

The mode of the collected data corresponds to the answer with the highest frequency (i.e. most repeated answer) (William and Robert, 2012).

3.4 Statistical Analysis and Discussion of Results

In this Section, the collected data from the survey corresponding to each topic (Appendix I) are statistically analyzed, along with a discussion of the findings. Specifically, the following results include the sample mean, standard deviation, standard error of the mean and the level of goodness.

3.4.1 Topic 1: Reactive and Proactive Services

Table 3 – 6 presents the statistical results of the questions pertaining to Topic 1. First of all it can be seen that the level of goodness for the answers to the questions are consistent and can be considered “Good”. This can be observed by considering the SEM, which is relatively small (around 0.1), except for the answers related to Question 4, which has an SEM of about 0.189. This is attributed to the relatively larger SD of about 1.134. Additionally, Question 6 is the only one with sample mean less than 4; while all the other questions have sample means greater than 4.

Table 3-6
: Summary of Results of Topic 1

Question Number	Sample Mean ± SD	SEM	Mode	Level of Goodness
1	4.528 ± 0.559	0.093	5	Good
2	4.556 ± 0.607	0.101	5	Good
3	4.167 ± 0.737	0.123	4	Good
4	4.028 ± 1.134	0.189	5	Good
5	4.500 ± 0.609	0.102	5	Good
6	3.861 ± 0.762	0.127	4	Good
7	4.556 ± 0.504	0.084	5	Good

With respect to the mode, it can be seen that Questions 3 and 6 are the only questions with the most repeated answer of "Agree (4)"; while all the other questions have the answer of "Strongly Agree (5)" as their most preferred choice. Generally speaking, most of the survey takers "Agree" or "Strongly Agree" that the reactive and proactive services are necessary for their organizations. Finally, Figure 3 – 1 graphically illustrates the sample mean and SD, which illustrates that Question 4 has the largest SD.

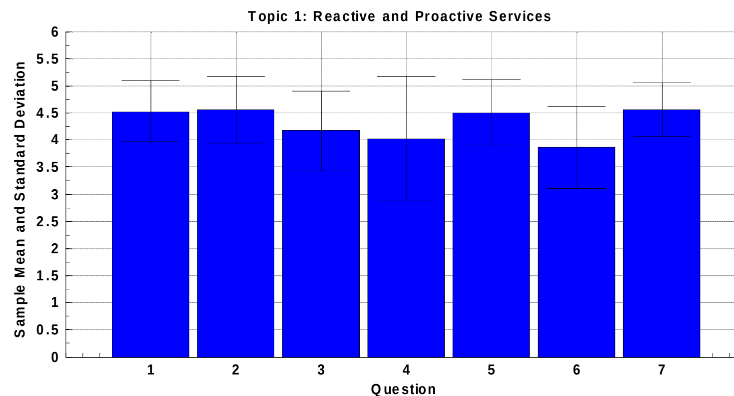


Figure 3-1
Sample Mean and Standard Deviation of Topic 1 Questions

3.4.2 Topic 2: Cyber-Attacks

In Table 3 – 7, the statistical results of the second topic are summarized. It is evident the answers to all the questions of this topic are consistent. Particularly, the sample means of all the questions are more than 4 (i.e. "Agree" or "Strongly Agree"). Additionally, the SD of each question is less than 1 (as also illustrated in Figure 3 – 2), and the mode of all questions is "Strongly Agree (5)", with the level of goodness being "Good".

Table 3-7
Summary of Results of Topic 2

Question Number	Sample Mean ± SD	SEM	Mode	Level of Goodness
8	4.417 ± 0.770	0.128	5	Good
9	4.667 ± 0.586	0.098	5	Good
10	4.444 ± 0.625	0.109	5	Good
11	4.611 ± 0.549	0.091	5	Good
12	4.639 ± 0.639	0.107	5	Good
13	4.556 ± 0.504	0.084	5	Good

Lastly, the SEM of each question is about 0.1 (i.e. relatively small). Hence, most of the surveyors agree that serious measures (i.e. plans and practices) must be implemented to counteract potential cyber-attacks.

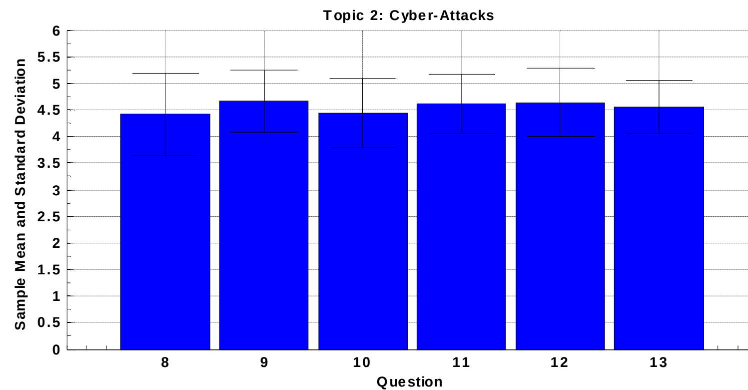


Figure 3-2
Sample Mean and Standard Deviation of Topic 2 Questions

3.4.3 Topic 3: Obstacles Impacting Information Security

In Table 3 – 8, one can see that the level of goodness of all the questions of Topic 3 are “Good”, except for Question 16, which shows a rather “Acceptable” level of goodness. This can be attributed to the sample mean corresponding to the value of 3.167. Also, the SD of that question is about 1.108, which is considered relatively high, resulting in an SEM of about 0.185. Moreover, the mode corresponding to that question is 2, which indicates that most survey takers disagree with the statement that there are no national experts in the field of information technology (Appendix I, Topic 4). This can also be seen from Figure 3 – 3, which clearly shows that Question 16 has the largest standard deviation and lowest sample mean, when compared with the other questions.

Table 3-8
Summary of Results of Topic 3

Question Number	Sample Mean ± SD	SEM	Mode	Level of Goodness
14	3.944 ± 0.893	0.149	4	Good
15	3.694 ± 0.980	0.163	4	Good
16	3.167 ± 1.108	0.185	2	Acceptable
17	4.333 ± 0.793	0.132	5	Good
18	4.500 ± 0.811	0.135	5	Good
19	3.917 ± 0.937	0.156	4	Good
20	4.250 ± 0.806	0.134	4	Good

In general, most of the survey takers agree that there is not a clear set of strategies, laws or legislation to protect information systems in Kuwait. Therefore, it is essential that KW-CERT implement and augment law enforcement procedures and legislations.

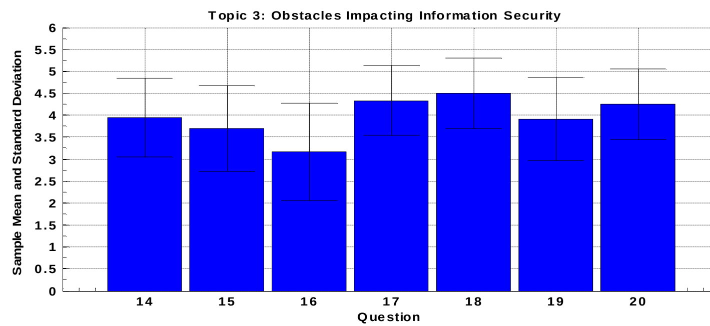


Figure 3-3
Sample Mean and Standard Deviation of Topic 3 Questions

3.4.4 Topic 4: Security Awareness

Table 3 – 9 summarizes the statistical results of the survey questions of Topic 4. As for the level of goodness, one can see that the responses of the survey takers are rather divided; some are "Good" while the rest are "Acceptable". Particularly, all the questions with "Acceptable" level of goodness have sample means that are below 3.67. Also, Question 22 has the lowest sample mean, with its mode being 3 (i.e. "Neutral"). This implies that the surveyees are rather divided with respect to their organizations holding regular security sessions (Appendix I, Topic 5).

Table 3-9
Summary of Results of Topic 4

Question Number	Sample Mean ± SD	SEM	Mode	Level of Goodness
21	3.694 ± 1.215	0.202	4	Good
22	3.139 ± 1.125	0.186	3	Acceptable
23	3.194 ± 1.305	0.217	4	Acceptable
24	3.417 ± 1.360	0.227	4	Acceptable
25	3.611 ± 1.128	0.188	4	Acceptable
26	3.194 ± 1.327	0.221	4	Acceptable
27	4.222 ± 0.959	0.159	4	Good
28	3.778 ± 1.149	0.192	5	Good
29	4.222 ± 0.832	0.139	4	Good
30	3.861 ± 1.268	0.211	5	Good
31	3.333 ± 1.042	0.174	4	Acceptable
32	3.472 ± 1.276	0.213	4	Acceptable

Moreover, it is only Question 30 that shows consensus in terms of answers, with the mode being “Strongly Agree (5)”. Finally, it is noticed that most of the questions in this topic have relatively high SD values (and hence SEM values), which implies that there is a high variance in the views of the survey takers, when it comes to security awareness in their organizations.

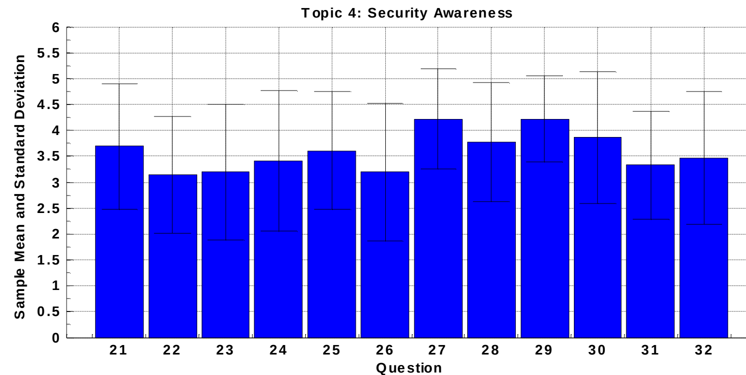


Figure 3-4
Sample Mean and Standard Deviation of Topic 4 Questions

3.4.5 Topic 5: Handling Security Threats

The statistical results of the questions pertaining to Topic 5 are given in Table 3 – 10. It can be seen that only Question 33 is considered “Good”; while the rest are considered “Acceptable”. Additionally, the last four questions have SEM values that are above 0.150, which is indicates relatively high SD values. Moreover, Question 35 seems to have the lowest sample mean and its mode is 3, which indicates that most of the survey takers are rather neutral with respect to their knowledge of whether threat-

related information is being exchanged between governmental and private entities (Appendix I, Topic 6).

Table 3-10
Summary of Results of Topics 5

Question Number	Sample Mean ± SD	SEM	Mode	Level of Goodness
33	3.861 ± 0.899	0.149	4	Good
34	3.611 ± 0.964	0.161	4	Acceptable
35	3.028 ± 1.276	0.213	3	Acceptable
36	3.472 ± 1.253	0.209	5	Acceptable
37	3.139 ± 1.150	0.192	4	Acceptable

Figure 3 – 5 corroborates the summarized results. Finally, one can see that the survey takers are not sure about their organizations' threats and security handling procedures, and whether there are clear policies for security threats.

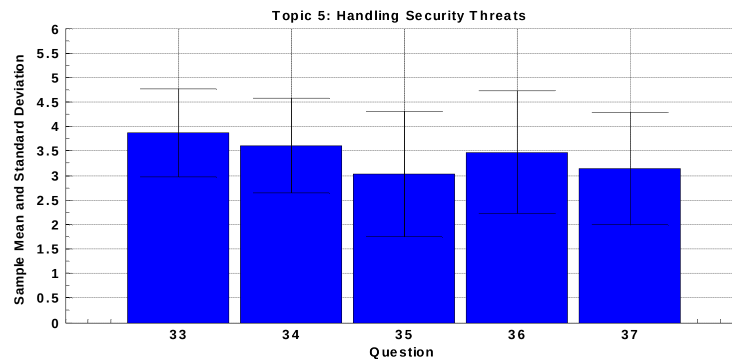


Figure 3-5
Sample Mean and Standard Deviation of Topic 5 Questions

3.5 Conclusions

In this Chapter, the statistical results and findings of the survey related to the security services, threats and awareness in Kuwait have been presented. Particularly, five different topics have been included in the survey, with a total of 37 questions and five possible answers to each question. It has been demonstrated that when it comes to the need of reactive and proactive services, there is consensus that such services should be widely implemented in both the governmental and private sectors, with the need for raising awareness to incident response and handling. As for cyber-attacks, there is a general agreement that a strategic plan should exist along with the best practices to counteract cyber-attack threats. In other words, it is undeniable that there should be specific security related plans, procedures and practices to handle any security-related attacks in Kuwait. On the other hand, most of the survey takers have agreed that there are obstacles impacting information security in Kuwait, since there are no clear

national laws, procedures or legislation that protects governmental and private information systems. Additionally, most of the surveyors agree that there is not enough awareness when it comes to security policies and procedures in their organizations. Also, there is a lack of proper training and education to the best practices for physical security. Finally, there is an agreement on the need for specific procedures to combat the security threats and ensure that both employees in the governmental and private sectors receive proper technical and event handling training.

Chapter 4
Implementation and Operations of KW-CERT

4.1 Introduction

The study in the previous chapter has brought forward in-depth insights into the issues that need to be taken into consideration and hence implemented in KW-CERT. However, it should be noted that there is not a specific list of guides as how to establish KW-CERT. This is because its establishment is driven by the needs of the different governmental and private organization as well as the sensitivity of the data. Moreover, there may be opportunities to derive some common goals and steps towards success from the number of guides currently available, and share those among the different organizations. Therefore, there is a common understanding of what KW-CERT should be; involving successful communication, cooperation, training, development and dissemination of good practices.

This Chapter outlines the responsibilities and operations of KW-CERT. Particularly, light will be shed on the necessary steps, components and services that must exist in KW-CERT to succeed.

4.2 Cooperation and Trust

With the growth of Internet connections and applications around the world, cyber-security issues may not be mitigated within a single country. This means that methods and tools of mitigation have become common practice. At the same time, cyber threats are becoming more numerous, diverse and sophisticated, which poses the need to adapt to a new challenge on daily basis. Therefore, it is essential to build and keep trust between different organizations and countries around the globe. Additionally, facilitating communication, establishing or participating in trust networks and communicating externally are some of the key roles expected from KW-CERT in a crisis situation or major incident (ENISA, 2009).

There may be different security teams within different organizations. However, their goals, constituency, and services may differ. Therefore, there must be some sort of collaboration in the form of exchanging information within their organization and others outside of it. Therefore, there must be vision and determination for the success of KW-CERT.

Many CERTs around the world mitigate incidents and respond to emergencies on a daily basis, and are successful in their work. They do so in collaboration with many different CERT partners. There are several formal and information partner ships that have proven to be a success. However, these partner ships are not easily obtained, due to regional difference in budgets and priority settings. Hence, it is essential to pave the

way for KW-CERT to connect to other CERTs around the globe and form trusted networks for information exchange and up-to-date practices.

Another issue is the trust level KW-CERT can establish and maintain within its constituency and its college CERTS (nationally and internationally), which will determine whether the services of KW-CERT are used and/or accepted. It is undeniable that KW-CERT's work is extremely sensitive for many reasons. First, it involves vulnerabilities, reputations or private/sensitive data that have to be exchanged to mitigate cyber incidents or threats. In turn, this requires work on building high levels of trust between national as well as international agencies and individuals. Thus, trust is the basis of cooperation, and developing ideas and solutions together. Second, there is a need to engage with stakeholders to take away misunderstandings about the way KW-CERT works, so as to eliminate any ill-advised decisions that ultimately lead to a break in trust and thus an end to any potential cooperation between KW-CERT and international CERTS as well as local agencies (ENISA, 2006**)**.

4.3 Main Responsibilities

The main responsibilities of KW-CERT consist of the external services it provides to its constituency, and its internal support processes (ENISA, 2009).

4.3.1 Incident Handling

It is undeniable that 100% cyber-security does not exist without an effective incident handling capability, attacks and intrusions on critical national information infrastructure could cripple the state for the duration of the attack. Consequently, handling cyber-security incidents and incidents related to critical information infrastructure (CII) (e.g. public communication networks or financial services), are a priority for KW-CERT. Incidents related to CII can pose a direct threat to society and the lives of the people living in Kuwait. These incidents should therefore receive priority over all ongoing activities and be contained and mitigated as quickly as possible (Killcrece and Ruefle, 2008) and (ENISA, 2009).

4.3.2 National Point of Contact for Incident Reporting and Information Dissemination

KW-CERT should act as the national point of contact for reports on incidents and the dissemination of security-related information. This task should be well-defined in order to achieve clear and flexible national and international collaboration. Foreign CERTs must clearly know whom to contact with regards to the sharing of security-related information and the reporting of incidents. Additionally, KW-CERT should be best-positioned to further disseminate such information (alerts, warnings, announcements,

vulnerabilities, etc.) among other CERTs in the world and information security communities (Control and Protection of National Information Technology Infrastructure, 2011).

4.3.3 Critical Information Infrastructure Protection (CIIP)

Services may be provided in addition the incident handling services and being the point of contact, this may include risk analysis, security consulting, security assessment, intrusion detection services and many other services. In addition to these services, KW-CERT should provide services such as (Center for Security Studies, ETH Zurich, 2007):

1. Announcements informing constituents about new developments with medium-to-long-term impact, such as newly found vulnerabilities.
2. Security-related information sharing that provides constituents with a comprehensive and easy-to-find collection of useful information and guidelines for improving security.
3. Alerts and warnings involving the dissemination of information that describes an intruder attack, security vulnerability, intrusion alert, computer virus or hoax.
4. Provide a short-term recommended course of action for dealing with the resulting problem.
5. Awareness building that provides information and guidance for conforming better to accepted security practices and organizational security policies.

These services deliver great value to the constituency in an efficient manner, as the information needed to provide these core services can be leveraged for the entire constituency. Moreover, security notification and other information for the constituents also greatly improve the visibility and the standing of KW-CERT, and facilitate the building of trust in the capabilities of KW-CERT (Center for Security Studies, ETH Zurich, 2008).

4.4 Proposed Steps for Successful Implementation

The following steps are proposed for successful implementation of KW-CERT (Carnegie Mellon University SEI – CERT Coordination Center, 2007).

4.4.1 Misconceptions of Functions and Tasks of KW-CERT

It is no surprise that misconceptions lead to misunderstandings that can seriously influence the performance of a CERT. Therefore, cooperation and development of the KW-CERT in different parts of the government is an area that needs further development and consideration. Moreover, there may be several strong misconceptions on, for instance, what KW-CERT is and does or does not do. Furthermore, the inner workings of KW-CERT may not always be clear to (governmental or private) organizations setting

or planning cyber security policy at a national level. This is turn suggests that there is a need to identify better ways of defining good practices and standards on what KW-CERT does, and advocate these to relevant organizations.

4.4.2 Mitigation of Incidents Involves Sharing of Sensitive Data

There is urgency in discussing this topic further with governmental and private regulatory agencies; probably with the participation of other stakeholders facing the same challenge. The key here is to engage in and intensify the dialogue with government and agencies (Institute for Information Infrastructure Protection, 2009).

4.4.3 Implementation of Good Standards

Clearly, there is a need for swifter implementation of Internet standards and good practices in general and in KW-CERT in particular.

4.4.4 Mandatory Cooperation with Law Enforcement and Other Regulatory Agencies

It is essential that KW-CERT to collaborate with law enforcement agencies (LEAs) and establish punishments for cyber-security related violations. The work of KW-CERT is delicate and involves working with private and sensitive data. Often, a cyber incident cannot be mitigated without handling and sharing this data with other CERTs and KW-CERT's own constituents in order to protect ICT systems and the individual persons involved in the incident and who are behind the ICT systems. Therefore, when drafting legislation, whether on KW-CERT's or on privacy, an acknowledgment of such delicacies involved in the execution of the tasks and operations of KW-CERT must be made. Additionally, KW-CERT should maintain a good working relationship with privacy regulators, as they both contribute to similar goals (Carnegie Mellon University SEI – CERT Coordination Center, 2007).

The current national laws (or the lack of them) on privacy and data exchange may prevent KW-CERT from formally sharing data with other CERTS, industry, law enforcement or regulatory agencies. Therefore, for necessary future implementation of KW-CERT, it is important to find out the difference between perceptions and legal reality. Furthermore, it is suggested that KW-CERT open up to other stakeholders, for the current laws to be thoroughly studied, potentially changing perceptions to realistic legislations. In addition, the issue of sharing privacy relevant information and under which safeguards or controls this is acceptable or not, should be addressed in a partnership between KW-CERT, privacy regulators and law enforcement agencies. Hence, KW-CERT and its constituents must ensure

to follow applicable law and adhere to privacy expectations (Institute for Information Infrastructure Protection, 2009).

4.4.5 Education, Training and Participating in International Meetings

It is essential the all the IT experts working with KW-CERT receive proper education and training, both nationally and internationally.

4.4.6 Development of Case Studies

There is a need for extensive case studies for serious cyber-security incidents and any lessons learned to be thoroughly studied, analyzed and reported with relevant stakeholders.

4.4.7 Data Feeds

Data feeds provide information on malware infections or other incidents across the CERT's constituency. Such data can be collected through a number of means; for instance, through the analysis of malicious code samples, or monitoring of active attacks on a network.

4.5 Cost of Building KW-CERT

The cost of building KW-CERT will vary, depending on the devices, tools and software that need to be bought from international vendors. The highest cost within KW-CERT will usually be the employee's wages, and ultimately on the size of KW-CERT, the size of the constituency, and the services KW-CERT wishes to offer. Additional costs may be imposed due to import restrictions on (for instance) certain crypto features. However, at this point, it is difficult to determine the number of individuals working under KW-CERT and the size of the networks or constituencies it protects. Lastly, the costs for training the staff, maintenance as well as travel costs must be taken into consideration.

4.6 Security Quality Management Services

Security quality management services are related to the security management processes of the constituents, particularly where KW-CERT can provide specific and consistent support in, for example, security awareness building, CIIP business continuity or risk analysis. KW-CERT can use and aggregate the output of the reactive and proactive services (see Chapter 3) it delivers for all its constituents regarding, for instance, the most frequently reported incidents and newly discovered vulnerabilities. Moreover, KW-CERT should have the authority and the breadth to reach all relevant domestic organizations and the country's population (Center for Security Studies, ETH Zurich, 2008).

The most important security quality management services that should be considered for delivery by KW-CERT are the following (ENISA, 2009):

1) *Awareness Building:* KW-CERT has an important role in advancing security knowledge and awareness, both within government and critical information infrastructure organizations, as well as within the general public. Most CERTS publicize awareness materials concerning, for instance, password best practices and phishing protection. As humans are often considered one of the weakest links in cyber-security, awareness building is a very important objective.
2) *Education and Training:* Through workshops, courses, tutorials or exercises, KW-CERT may provide their constituents with information and training on various topics, such good practices in incident or vulnerability management.
3) *Business Continuity Management (BCM) and Disaster Recovery Planning (DRP):* It is undeniable that BCM/DROP is a key aspect of any plan for CIIP. Therefore, KW-CERT should be involved in the cyber-security aspects of the business continuity and disaster recovery management processes for their constituents.
4) *Risk Management:* Through knowledge of the environments and information collected via the reactive (incident, vulnerability, and artifact handling) and proactive (intrusion detection service and security assessment) services, KW-CERT can build a snapshot of the situational awareness in its constituency.

4.7 Operations

One must acknowledge that for a successful implementation and operation of KW-CERT, there is a vast need for appropriate people, technology and processes. Without operational resources, such as staff and infrastructure, KW-CERT cannot offer the reactive and proactive services discussed in Chapter 2. Additionally, the operational capabilities and requirements that enable KW-CERT to provide services of adequate quality to its constituency must also be studied (Institute for Information Infrastructure Protection, 2009).

The operation of KW-CERT is unique because it will be required to continue operating under all circumstances. In turn, it is essential to consider the following four operational aspects discussed in the upcoming subsections.

4.7.1 Human Resources

This is dependent on the governmental budget (i.e. funding) assigned to KW-CERT, regulatory and business drivers, business hours, etc. Therefore, building a successful KW-CERT requires building the right *team* and associating it with a well-defined set of *operations*, as detailed in the following subsections (Center for Security Studies, ETH Zurich, 2008).

4.7.1.1 Team

The KW-CERT team must consist of the following team members (Carnegie Mellon University SEI – CERT Coordination Center, 2007):

1) *Team Leader/Manager/Coordinator:* The role of the team leader is to provide strategic direction, and supervise the team; in addition to his/her role as the authoritative representative of KW-CERT.
2) *Incident Handlers:* These people provide incident-handling capability, by monitoring, analyzing, and responding to incidents. In addition, they take on the responsibility of technology watch, the dissemination of information and other tasks when no incidents are ongoing.
3) *Technical Experts:* The technical experts are responsible for vulnerability handling, writing of technical reports, training, support of specific platforms, and security assessment services.
4) *Support Staff:* These are the team members of carry out administrative tasks, monitor reports on events and incidents, and are responsibility for the dissemination of information.

Cyber-security knowledge and communications skills are the most essential competences of a KW-CERT employee.

4.7.1.2 Operations

It is should be noted that the main operation of KW-CERT is both working for the protection of the critical information infrastructure of the governmental and private sectors and for all incidents in its constituency. Undeniably, it should be considered obligatory for KW-CERT to be reachable 24 hours a day, 7 days a week, and 365 days a year (24/7/365), by its constituents, and its national and international partners. Specifically, international cooperation and timely incident response will prove a challenge because of time differences. Therefore, depending on the service portfolio, work structure and responsibilities, the team will need to be reachable either physically or through "on-call" duty (The Center for Internet Security, 2010).

In summary, the following is needed in terms of human resources:

1. Adequate and appropriate human resources should be dedicated to supporting the operation of KW-CERT.
2. The human resources that are dedicated to the operation of KW-CERT need to have appropriate skills and expertise, which requires adequate investment.
3. Hiring adequate staff and making provision for ongoing staff training and exercises.

4.7.2 Infrastructure

KW-CERT must possess the following components as part of its infrastructure (Center for Security Studies, ETH Zurich, 2008).

4.7.2.1 Communication Services

KW-CERT may not necessarily have direct access to the systems affected by an incident; therefore, the team will rely on its communication services to receive information about the incident, in order to analyze it, and to coordinate the handling of the incident. Additionally, this reliance on communication services is true for almost all services under the umbrella of KW-CERT. In order to exchange information security, KW-CERT should provide the contact details for signed and encrypted email. In addition, the team's website should provide a security means of communications (e.g. an http-protected incident reporting form).

4.7.2.2 Logical Security

In addition to the security measures for communication channels, logical security controls should be implemented to protect the confidentiality and integrity of information. This can be done by means of (Center for Security Studies, ETH Zurich, 2008):

1) An internal information security management framework and policy in order to provide the security strategy and authorization to implement controls over the information classification scheme (shared with the constituency and partners in cooperation), password policy, and access management policy.
2) Integrity control to prevent unauthorized changes.
3) Confidentiality controls, such as encryption.

More importantly, all logical security measures should be managed by KW-CERT itself, so as to ensure confidentiality and integrity.

4.7.2.3 Physical Security

As KW-CERT naturally deals with sensitive information that needs to be protected, adequate measures must be taken to physically secure the premises of a team.

The following pointers should be taken into consideration when implementing the infrastructure of KW-CERT (Center for Security Studies, ETH Zurich, 2008):

1) Ensure high availability of their communication services by avoiding single points of failure and have at least several means for being contacted and for contacting others.
2) Security measures to ensure the confidentiality and integrity of information in transit (secure email, https) and at rest (encryption, access control) should be implemented and managed by KW-CERT.

3) KW-CERT should be secure in every way, not only logically but also in the physical sense. The offices and the supporting information systems must be located in secure sites.

4.7.3 Provision of Services

KW-CERT should ensure the efficiency and effectiveness of the services it delivers. Particularly, it should identify and monitor their most important key performance indicators (KPIs) in order to evaluate the quality and performance of their services. The indicators should be relevant to KW-CERT's mission objectives and weighted according to the importance of the services to which they relate.

The general KPIs are (The Center for Internet Security, 2010):

1) Response times for service events (e.g. incident, vulnerability report) and/or priority scheme.
2) Level of information provided for service events (short-term).
3) Time-to-live for service events.
4) Level of information provided on the longer term (e.g. reports, summaries, announcements, etc.).

Several supporting processes and tools could increase the efficiency and maturity of service delivery. For instance, KW-CERT must follow-up with a constituent within two working days of the initial report. This should be part of KW-CERT's supporting process on the follow-up time on vulnerability reports for all non-urgent vulnerabilities. As for high-priority incidents, every high priority incident should be acknowledged within two hours. Moreover, analysis should start within the first hour of receipt of such a report.

An essential tool for service delivery is an incident recording and tracking systems (also known as ticketing system). In turn, this will allow the creation of tickets that are associated with incidents. Moreover, during the incident handling phases, the ticket will be enriched with information, ensuring a formal audit trail and log of the incident.

To ensure that all incidents are attended to, a workflow management system can queue and centralize information coming via different communication channels, and it should allow predefined workflows to be followed in the handling of incidents. This in turn should allow proper monitoring of the status of various incidents, facilitates the hand-over between shifts, generates reports, and ensures standard processes are executed.

4.7.4 Business Continuity

KW-CERT should possess a solid plan for service continuity. Having and demonstrating this ability directly reflects on the perceived competence and level of trust its constituency has in it. Ensuring continuity

covers many important aspects of operations. For instance, managing incoming requests and the ability to correctly distribute them among staff is one of these aspects. Moreover, a 24/7/365 operational mode should allow constituents to call in reports anytime. Also, the ability to cope with the unavailability of critical communication channels and operational elements such as email or information servers is of paramount importance. This is to eliminate the inability to provide specific services in a timely manner, as they could lead to failure in meeting contractual requirements and/or services, as specified in service level agreements. Hence, this needs to be avoided as much as possible by a redundant and resilient infrastructure and a variety of communications channels, as discussed earlier. Lastly, KW-CERT must provide on-going training to staff to ensure that they possess up-to-date knowledge and regular exercises (Institute for Information Infrastructure Protection, 2009) and (The Center for Internet Security, 2010).

Finally, a few last pointers are worth mentioning to ensure the continuity of KW-CERT. First, a proper system for managing and routing various requests must be implemented in order to facilitate handovers. Second, full-time staffing is essential for KW-CERT to ensure availability at all times. Lastly, to ensure the continuity of any critical information infrastructure, redundant systems and backup working space should be set up to ensure access to the means of communication in the face of attacks and/or system failures.

4.8 Conclusions

The services offered by KW-CERT will determine the tools it needs in order to be effective. At this point, it is impossible to come up with one comprehensive standard list. In its current state and without any tools, KW-CERT cannot cooperative effectively with its constituency or with its peers.

4.9 Summary and Future Work

4.9.1 Summary

Based on this study the following critical recommendations can be made:

1. KW-CERT must minimally provide an effective incident handling capability for its constituents. Moreover, handling cyber-security incidents on a national or cross-border scale, and incidents related to critical information infrastructure (CII), should be the absolute priority of KW-CERT.
2. KW-CERT should also provide the core proactive services (i.e. alerts, warnings, announcements and the dissemination of security-related information).
3. KW-CERT must also reduce the severity of cyber-security incidents by providing proactive assistance in securing the constituency's

infrastructure. This can be provided to the entire constituency at the same time, so that the effort and cost involved are kept relatively low.

4. KW-CERT should provide its constituents with more advanced education and training on the best practices in cyber-security.
5. Sufficient staff and resources must be provided so that KW-CERT can be integrated efficiently with other services.
6. KW-CERT should be actively involved in business continuity management and disaster recovery planning for national CIIs. Moreover, it should strive to build a capability in dynamic risk analysis (situational analysis) concerning the country’s CIIs.
7. Although most of Kuwait's governmental and private organizations’ employees have IT related degrees, it is essential that they receive proper training and education on the security-related policies and procedures.
8. Build broad public awareness of the risks associated with online activities using public awareness campaigns on cyber-security.
9. Before a seccessful KW-CERT can be built, misconceptions of functions and tasks must be cleared via cooperation and practice among KW-CERT employees.
10. Adequate and skillful human resources must be hired and assigned to different sensitive operations while ensuring proper communication and collaboration between the different entities.
11. Integrate law enforcement and other regulatory agencies to KW-CERT's policies and regulations.

4.9.2 Future Work

There are several research directions that may be considered in the future as an extension of this study. These can be summarized as follows:

1. Building the organizational structure of KW-CERT along with the different teams, departments, management and authorities.
2. Designing network architecture of KW-CERT so that the different governmental and private organizations in Kuwait can be connected.
3. Supporting KW-CERT, including hiring, training of staff, purchasing software and hardware, testing and installation of connections.
4. Perform budget analysis for managing people and handling of resources with financially quantifiable responsibilities.

References

ABI Research. (2013). **More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020**. Avalabile at: https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne (Last Accessed: Apr. 15, 2016)

Asia-Pacific Computer Emergency Response Team (APCERT). (2014). **About APCERT**. Avalabile at: http://www.apcert.org/about/index.html (Last Accessed: Apr. 15, 2016)

Australia Computer Emergency Response Team (AusCERT). (2010). **About AusCERT**. Avalabile at: https://www.auscert.org.au/main/about (Last Accessed: Apr. 15, 2016)

Australian Government – CERT Australia. (2015). **About Us**. Avalabile at: https://www.cert.gov.au/about (Last Accessed: Apr. 15, 2016)

Boyce, J. and Jennings, D. (2002). **Information Assurance: Managing Organizational IT Security Risks**. Oxford: Butterworth-Heinemann (Elsevier).

Brazilian National Computer Emergency Response Team (CERT.br). (2014). **About CERT.br**. Avalabile at: http://www.cert.br/en/ (Last Accessed: Apr. 15, 2016)

Buyya, R., Broberg, J., and Goscinski, A. (2011). **Cloud Computing: Principles and Paradigms**. Hoboken, New Jersey: Wiley and Sons, Inc.

Carnegie Mellon University SEI – CERT Coordination Center. (2007). **Incident Management Capability Metric**. Avalabile at: http://www.cert.org/archive/pdf/07tr008.pdf (Last Accessed: Apr. 15, 2016)

Center for Security Studies, ETH Zurich. (2007). **A Generic National Framework for Critical Information Infrastructure Protection (CIIP)**. Avalabile at: http://www.itu.int/osg/spuold/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf (Last Accessed: Apr. 15, 2016)

Center for Security Studies, ETH Zurich. (2008). International CIIP Handbook 2008/2009 – An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies.

Avalabile at: http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf (Last Accessed: Apr. 15, 2016)

Cloud Computing in India. (2013). **Cloud Computing**. Avalabile at: http://www.cloudcomputingindia.co.in/ (Last Accessed: Apr. 15, 2016)

Control and Protection of National Information Technology Infrastructure. (2011). **Terms of Reference for Consultancy Services for Central Agency for Information Technology (CAIT)**.

ENISA. (2006**). CERT Cooperation and Its Further Facilitation by Relevant Stakeholders**. Avalabile at: http://www.enisa.europa.eu/act/cert/background/coop (Last Accessed: Apr. 15, 2016)

ENISA. (2009). **Analysis of Member States' Policies and Regulations – Policy Recommendations**. Avalabile at: https://www.enisa.europa.eu/publications/archive/analysis-of-policies-and-recommendations/at_download/fullReport (Last Accessed: Apr. 15, 2016)

ENISA. (2009). **Baseline Capabilities for National/Governmental CERTS**. Avalabile at: http://www.enisa.europa.eu/act/cert/support/baseline-capabilities (Last Accessed: Apr. 15, 2016)

ENISA. (2012). **Roadmap to Provide More Proactive and Efficient CERT Training**. Avalabile at: https://www.enisa.europa.eu/activities/cert/support/exercise/roadmap-to-provide-more-proactive-and-efficient-cert-training (Last Accessed: Apr. 15, 2016)

ENISA. (2013). **Alerts, Warnings and Announcements - Best Practices Guide**. Avalabile at: https://www.enisa.europa.eu/activities/cert/support/awa (Last Accessed: Apr. 15, 2016)

ENISA. (2015). **Recommendations on Baseline Capabilities**. Avalabile at: https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities(Last Accessed: Apr. 15, 2016)

European Union Agency for Network and Information Security (ENISA). (2005). **About ENISA**. Avalabile at: http://www.enisa.europa.eu/about-enisa (Last Accessed: Apr. 15, 2016)

FCC. (2001). **Computer Security Incident Response Guide**. Avalabile at:

http://www.iwar.org.uk/comsec/resources/fasp/Incident-Response-Guide.pdf (Last Accessed: Apr. 15, 2016)

Forum of Incident Response and Security Teams (FIRST). (2014). **About FIRST**. Avalabile at: http://www.first.org/about (Last Accessed: Apr. 15, 2016)

IBM. (2015). **The Internet of Things**. Avalabile at: http://www-01.ibm.com/software/info/internet-of-things/ (Last Accessed: Apr. 15, 2016)

ictQatar. (2005). **About Qatar Computer Emergency Response Team (Q-CERT)**. Avalabile at: http://www.qcert.org/ (Last Accessed: Apr. 15, 2016)

Institute for Information Infrastructure Protection (I3P). (2009). National Cyber Security Research and Development Challenges – Related to Economics, **Physical Infrastructure and Human Behavior**. Avalabile at: https://www.fbiic.gov/public/2009/feb/i3pnationalcybersecurity.pdf (Last Accessed: Apr. 15, 2016)

Intel IT Center. (2013). **Planning Guide: Virtualization and Cloud Computing**. Avalabile at: http://www.intel.com/content/dam/www/public/us/en/documents/guides/cloud-computing-virtualization-building-private-iaas-guide.pdf(Last Accessed: Apr. 15, 2016)

Internet Governance Forum (IGF). (2014). **Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security**. Avalabile at: https://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file (Last Accessed: Apr. 15, 2016)

Internet of Things Council. (2015). **The Internet of Things**. Avalabile at e: http://www.theinternetofthings.eu/what-is-the-internet -of-things (Last Accessed: Apr. 15, 2016)

IT Law Wikia. United States Computer Emergency Readiness Team. Avalabile at: http://itlaw.wikia.com/wiki/United_States_Computer_Emergency_Readiness_Team (Last Accessed: Apr. 15, 2016)

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC). (2003). **About JPCERT/CC**. Avalabile at: https://www.jpcert.or.jp/english/ (Last Accessed: Apr. 15, 2016)

Killcrece, G., and Ruefle, R. (2008). **Creating and Managing Computer Security Incident Handling Teams**.

Avalabile at: https://www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf (Last Accessed: Apr. 15, 2016)

Kruidhof, O. (2014). Evolution of National and Corporate CERTs - Trust, the Key Factor. In ***Best Practices in Computer Network Defense: Incident Detection and Response***. IOS Press. Avalabile at: https://www.nl.capgemini.com/resource-file-access/resource/pdf/olaf_kruidhof_-_evolution_of_national_and_corporate_certs.pdf(Last Accessed: Apr. 15, 2016)

Lewis, M. (2008). **Incident Management: ITU Pillars and Qatar Case Study**. Avalabile at: http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incident-management-brisbane-july-08.pdf (Last Accessed: Apr. 15, 2016)

Microsoft TechNet. (2015). **Common Types of Network Attacks**. Avalabile at: http://technet.microsoft.com/en-us/library/cc959354.aspx (Last Accessed: Apr. 15, 2016)

Q-CERT. (2007). **A National CERT – What Can It Do For You**? Avalabile at: http://www.menog.org/presentations/menog-2/ian-m-dowdeswell-regional-cert.pdf(Last Accessed: Apr. 15, 2016)

SANS Institute. (2001). **Computer Incident Response Team**. Avalabile at: https://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641(Last Accessed: Apr. 15, 2016)

Schultz, E. E., and Shumway, R. (2001). Forming and Managing an Incident Response Team. In ***Incident Response: A Strategic Guide to Handling System and Network Security Breaches***. Sams Publishing. Avalabile at: http://ptgmedia.pearsoncmg.com/images/1578702569/samplechapter/1578702569.pdf (Last Accessed: Apr. 15, 2016)

SRI Consulting Business Intelligence. (2014). **The Internet of Things Roadmap**. Avalabile at: http://www.trumpiot.co/2014/03/14/sri-consulting-business-intelligence-the-internet-of-things-roadmap/ (Last Accessed: Apr. 15, 2016)

Telecommunications Regulatory Authority of the UAE. (2009). **aeCERT at a Glance**. Avalabile at: http://www.tra.gov.ae/default.aspx (Last Accessed: Apr. 15, 2016)

TF-CSIRT Trusted Introducer. (2014). **Team Database**. Avalabile at: http://www.trusted-introducer.org/directory/country_LICSA.html (Last Accessed: Apr. 15, 2016)

The Center for Internet Security. (2010). **The CIS Security Metrics**. Avalabile at: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf (Last Accessed: Apr. 15, 2016)

The Central Agency for Information Technology (2006). **About CAIT**. Avalabile at: https://www.cait.gov.kw/About-Us/Amiri-Decree.aspx (Last Accessed: Apr. 15, 2016)

The Organization of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT). (2014). **Mission Statement**. Avalabile at: http://www.oic-cert.org/en/missionstatement.html (Last Accessed: Apr. 15, 2016)

The Report: Emerging Qatar. (2007). Oxford Business Group.

Trans-European Research and Education Networking Association (TERENA). (2014). **TF-CSIRT: Goals of the Task Force**. Avalabile at: http://www.terena.org/activities/tf-csirt/ (Last Accessed: Apr. 15, 2016)

United Arab Emirates – Computer Emergency Response Team (aeCERT). (2015). **Telecommunications Regulatory Authority**. Avalabile at: https://www.tra.gov.ae/aecert/ (Last Accessed: Apr. 15, 2016)

United States Computer Emergency Readiness Team (US-CERT). (2002). **About Us**. Avalabile at: https://www.us-cert.gov/ (Last Accessed: Apr. 15, 2016)

West-Brown, M. J., Stikvoort, D., Kossokowski, K.-P., Killcrece, G., Ruefle, R., Zajicek, M. (2003). **Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon Software Engineering Institute**. Avalabile at: http://www.sei.cmu.edu/reports/03hb002.pdf(Last Accessed: Apr. 15, 2016)

Wikipedia. (2014). **Computer Emergency Response Team**. Avalabile at: http://en.wikipedia.org/wiki/Computer_emergency_response_team(Last Accessed: Apr. 15, 2016)

William Mendenhall, Robert Beaver, (2012) **Introduction to Probability and Statistics**, 14th Ed., Duxbury Press.

Appendix (I)
KW-CERT Survey Questions

KW-CERT Survey Questions

Introduction to KW-CERT Survey

The Central Agency for Information Technology (CAIT) plans to establish a National Computer Emergency Response Team for the State of Kuwait (i.e. KW-CERT), which will be responsible for the protection of governmental and non-governmental administrative networks and national IT resources connected to the Cyberspace. It will act as a national point of contact for information sharing (like incident reports, vulnerability information and others) with other national CERTs existing worldwide. We will be very grateful if you can complete this survey, so that we can build a reliable CERT in Kuwait.

Name: ____

Occupation:

( ) Management
( ) Technical Support
( ) Operational
( ) Other

Sector:

( ) Government Sector
( ) Private Sector
( ) Other

Qualification:

( ) Bachelor (IT)
( ) Master (IT)
( ) PhD (IT)
( ) Other

Experience in IT:

( ) Less than 5 Years
( ) 6 - 15 Years
( ) More than 15 Years

Email Address: ______________________________________

Mobile Phone: ______________________________________

Topic 1

Reactive and Proactive Services

To what extent do you agree that the following services will be helpful to your organization?

1) Study the risks and threats faced by the region on a regular basis and develop methods to face them.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

2) Incident response and cyber risks response for both the governmental and non-governmental sectors.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

3) Issuing bulletins of awareness.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

4) Monitor the cyberspace of the country, social networking sites and private forums (i.e. underground community) for the possibility of the existence of information on any threats or possible operations of penetration points to the systems.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

5) Incident response and cyber risks response for both the governmental and non-governmental sectors.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

6) Incident response and cyber risks response to users of the internet at home.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

7) Development of educational programs in the field of cyber security to raise the level of awareness of cyber risks.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

---

Topic 2
Cyber-Attacks

To what extent do you agree on the following statements?

8) A strategic plan for information security should exist, and be extracted from national legislation to protect critical infrastructure.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

9) Apply best practices and ways to protect sensitive and critical information.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

10) Assess the readiness level of the states' organizations, especially the critical ones.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

11) Build capabilities and recruit experts in the field of information security.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

12) Early alarming systems should be deployed to reduce cyber-attack threats and take actions when discovered.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

13) Make researches and studies about the latest cyber-attack threats and how it can affect the organization.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

---

Topic 3

Obstacles Impacting Information Security

To what extent do you agree on the following statements?

14) There is no clear national strategy concerned with information security.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

15) There are no national laws or legislation that protects critical infrastructures.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

16) There are no national experts in the field of information technology.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

17) There is major reliance on vendors in technology usage and application.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

18) Security awareness should be provided to users who deal with critical information.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

19) The user is the weakest link in any information security system.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

20) There are no 100% preventive procedures for cyber-attack threats.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

---

Topic 4

Security Awareness

Do you agree/disagree on the following statements?

21) Our organization has a security awareness team.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

22) Your organization host regular security awareness training sessions.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

23) Your employees have a solid understanding of the organization's security policy, procedure and best practices.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

24) Employees connect their own devices or electronic gadgets to their work PC/Network .
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

25) None related work contents are downloaded at work.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

26) Non-technical employees have accessed areas of your IT system they should not have.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

27) Your organization has physical security (e.g. access codes to server rooms/cabinets).
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

28) Employees lock their computers when they walk away from them.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

29) Firewalls are used when accessing a wireless network in the workplace.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

30) A strong password or minimum password requirements is being in your organization.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

31) Your employees are aware of the importance of scanning any file they download from a website, email or online storage drives.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

32) Your employees are aware that illegal file sharing and downloading of copyrighted works can be a punishable offense.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

---

Topic 5

Handling Security Threats

Do you agree/disagree on the following statements?

33) Your data centers and servers handle events according to their severity.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

34) Events are assigned according to different risk/threat levels.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

35) Threat-related information is being exchanged with other governmental/non-governmental entities.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

36) There is a clear IT policy/procedure to reduce system downtime and network, or application outages.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

37) Your Organization has enough technical employees with privileged access, who have received proper training.
( ) Strongly Agree ( ) Agree ( ) Neutral ( ) Disagree ( ) Strongly Disagree

Appendix (II)
Additional KW-CERT Survey Results

Additional KW-CERT Survey Results

Question Number	Question	Percentage of Selection
1	Study the risks and threats faced by the region on a regular basis and develop methods to face them.	3% 0% 0% 42% 55% Strongly Agree Agree Neutral Disagree Strongly Disagree
2	Incident response and cyber risks response for both the governmental and non-governmental sectors.	6% 0% 0% 33% 61% Strongly Agree Agree Neutral Disagree Strongly Disagree
3	Issuing bulletins of awareness.	3% 0% 11% 33% 53% Strongly Agree Agree Neutral Disagree Strongly Disagree
4	Monitor the cyberspace of the country, social networking sites and private forums (i.e. underground community) for the possibility of the existence of information on any threats or possible operations of penetration points to the systems.	3% 11% 11% 44% 31% Strongly Agree Agree Neutral Disagree

5	Incident response and cyber risks response for both the governmental and non-governmental sectors.	5% 0% 0% 39% 56% Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
6	Incident response and cyber risks response to users of the internet at home.	6% 0% 17% 19% 58% Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
7	Development of educational programs in the field of cyber security to raise the level of awareness of cyber risks.	0% 0% 0% 44% 56% Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
8	A strategic plan for information security should exist, and be extracted from national legislation to protect critical infrastructure.	3% 0% 8% 33% 56% Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree

9	Apply best practices and ways to protect sensitive and critical information.	6% 0% 0% 22% 72% Strongly Agree Agree Neutral Disagree Strongly Disagree
10	Assess the readiness level of the states' organizations, especially the critical ones.	0% 0% 8% 39% 53% Strongly Agree Agree Neutral Disagree Strongly Disagree
11	Build capabilities and recruit experts in the field of information security.	3% 0% 0% 33% 64% Strongly Agree Agree Neutral Disagree Strongly Disagree
12	Early alarming systems should be deployed to reduce cyber-attack threats and take actions when discovered.	0% 3% 0% 28% 69% Strongly Agree Agree Neutral Disagree Strongly Disagree

13	Make researches and studies about the latest cyber-attack threats and how it can affect the organization.	0% 0% 0% 44% 56% Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
14	There is no clear national strategy concerned with information security.	0% 8% 28% 17% 47% Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
15	There are no national laws or legislation that protects critical infrastructures.	0% 14% 22% 25% 39% Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
16	There are no national experts in the field of information technology.	3% 14% 30% 25% 28% Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree

17	There is major reliance on vendors in technology usage and application.	
18	Security awareness should be provided to users who deal with critical information.	
19	The user is the weakest link in any information security system.	
20	There are no 100% preventive procedures for cyber-attack threats.	

21	Our organization has a security awareness team.	3% 22% 31% 8% 36% ■ Strongly Agree ■ Agree ■ Neutral ■ Disagree ■ Strongly Disagree
22	Your organization host regular security awareness training sessions.	8% 11% 20% 28% 33% ■ Strongly Agree ■ Agree ■ Neutral ■ Disagree ■ Strongly Disagree
23	Your employees have a solid understanding of the organization's security policy, procedure and best practices.	11% 20% 22% 25% 22% ■ Strongly Agree ■ Agree ■ Neutral ■ Disagree ■ Strongly Disagree
24	Employees connect their own devices or electronic gadgets to their work PC/Network.	11% 25% 20% 11% 33% ■ Strongly Agree ■ Agree ■ Neutral ■ Disagree ■ Strongly Disagree

25	None-related work contents are downloaded at work.	Strongly Agree 19%, Agree 47%, Neutral 14%, Disagree 14%, Strongly Disagree 6%
26	Non-technical employees have accessed areas of your IT system they should not have improvements.	Strongly Agree 19%, Agree 28%, Neutral 17%, Disagree 25%, Strongly Disagree 11%
27	Your organization has physical security (e.g. access codes to server rooms/cabinets).	Strongly Agree 42%, Agree 50%, Neutral 3%, Disagree 0%, Strongly Disagree 5%
28	Employees lock their computers when they walk away from them.	Strongly Agree 33%, Agree 31%, Neutral 19%, Disagree 14%, Strongly Disagree 3%

29	Firewalls are used when accessing a wireless network in the workplace.	6% 0% 8% 42% 44% — Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
30	A strong password or minimum password requirements is being in your organization.	8% 8% 11% 39% 34% — Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
31	Your employees are aware of the importance of scanning any file they download from a website, email or online storage drives.	3% 11% 22% 39% 25% — Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree
32	Your employees are aware that illegal file sharing and downloading of copyrighted works can be a punishable offense.	8% 25% 17% 19% 31% — Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree

33	Your data centers and servers handle events according to their severity.	0% 8% 25% 22% 45% ■ Strongly Agree ■ Agree ■ Neutral ■ Disagree ■ Strongly Disagree
34	Events are assigned according to different risk/threat levels.	3% 5% 14% 31% 47% ■ Strongly Agree ■ Agree ■ Neutral ■ Disagree ■ Strongly Disagree
35	Threat-related information is being exchanged with other governmental/non-governmental entities.	14% 17% 19% 17% 33% ■ Strongly Agree ■ Agree ■ Neutral ■ Disagree ■ Strongly Disagree
36	There is a clear IT policy/procedure to reduce system downtime and network, or application outages.	6% 19% 28% 25% 22% ■ Strongly Agree ■ Agree ■ Neutral ■ Disagree ■ Strongly Disagree

37	Your organization has enough technical employees with privileged access, who have received proper training.	Strongly Agree 11%, Agree 31%, Neutral 28%, Disagree 22%, Strongly Disagree 8%

المعلومات الشخصية

الاسم: محمد جاسم سعدون اليعقوب

التخصص: ماجستير الإدارة الهندسية

الكلية: الهندسة

السنة:2016م.

هاتف رقم: 0096567788007

البريد الإلكتروني: mohalyaqoub@gmail.com
al_yaqoub@yahoo.com